Securitas
Technology

2026
Global Technology Outlook Report

securitastechnology.com

Contents

Welcome & Thank You 04

About Securitas Technology 06

SecureStat® HQ™ Security Management Platform 08

1

Executive Summary 10

Key Takeaways 12

Data Trends & Insights 14

Partner Insights 18

2

Technology Trends to Watch in 2026 20

AI is Accelerating Everything 22

Cloud Applications as the New Normal 26

Advanced Sensor Applications Are Evolving 30

Action Plan for Security Professionals 34

3

Security Solutions for a Volatile Environment 36

Technology Improving Safety in all Environments 38

Strategies to Prepare Organizations & People 44

Securitas Group Insight: The Future of Crime Risk Intelligence 50

Action Plan for Security Professionals 52

4

Security Moving to Real-Time & Proactive Management 54

Augmenting the Agent with AI 56

Mining Data for Continuous Improvement 62

Securitas Group Insight: Augmenting the Officer 68

Action Plan for Security Professionals 70

5

Security Systems Driving Value & Organizational Impact 72

Security Data Contributing to Business Optimization 74

Promoting Sustainability & Streamlined Operations 80

Securitas Group Insight: Building a Culture of Employee Safety 86

Action Plan for Security Professionals 88

6

Technology Partner Profiles 90

Thank You to Our Contributing Strategic Partners

3xLOGIC
AMAG TECHNOLOGY An Allied Universal Company
ASSA ABLOY Opening Solutions
AXIS COMMUNICATIONS
BOSCH
brivo simply better security
DMP
EAGLE EYE NETWORKS
Genetec™
Hanwha Vision
HID
Honeywell
IDIS One Solution. One Company.
INTELLICENE UNIFYING SECURITY, ENABLING ACTION
MARCH networks A Delta Group Company
milestone
MOTOROLA SOLUTIONS
OpenEye
PACOM
resideo
Software House C·CURE IQ
SONITROL
VERINT
Viakoo

The world's leading technology manufacturers, innovators, and technologists.

Welcome & Thank You

Presenting the 2026 Global Technology Outlook Report

On behalf of all Securitas Technology associates worldwide, I'm delighted to welcome you to this, our eighth annual, Global Technology Outlook Report.

I want to begin by thanking our clients for their continued trust and partnership and for the insights that have shaped this year's report. I'd also like to thank our strategic partners and industry experts for their vital contribution; your expertise and passion for innovation are a driving force behind the report.

Our 2025 report was extremely well received by our clients and within the industry, complementing another landmark year for Securitas Technology. While we delivered tens of thousands of high-quality, end-to-end security projects for organizations worldwide, we continued to innovate – bringing new technologies, services, and benefits to our clients. Here are some highlights:

1. Launched our groundbreaking **sustainability initiative**, documenting data on security system power consumption and equivalent greenhouse gas emissions, building awareness, and offering clients choices for more sustainable security options.
2. Continued investment in our industry-leading security management digital platform, **SecureStat® HQ™**, adding new features and innovations to give clients more clarity and control over their security program.
3. Unveiled our new **Technician Apprentice Program**, developed in partnership with the Security Industry Association (SIA), signaling our dedication to developing the next generation of security professionals today.

Back with fresh information for 2026, this new edition of our Outlook Report is packed full of insights from the market, our strategic technology partners, industry technologists, and internal security experts across our global organization.

At Securitas Technology, we see our relationship with clients as more than just a service provider. We serve as a trusted advisor in security technology, helping clients stay ahead of the evolving trends and topics shaping the future of the security industry.

We're proud that our report has become a key fixture in the industry calendar, valued for its specific focus on technology trends within the electronic security space. The content within is designed to help you evaluate current and future market trends, anticipate emerging threats, understand emerging technologies, and confidently plan your organization's security roadmap and technology investments.

I invite you to explore each section of the report, including data-driven insights from our market survey, top technology trends to watch, latest innovations from our strategic partners, and expert advice on how your organization can prepare effectively for the future of security.

Tony Byerly
Global President & Chief Executive Officer
Securitas Technology

About Securitas Technology

A Global Technology Partner Solely Focused on Safety and Security

Across six continents, we offer a robust global infrastructure to deliver operational and service excellence, powered by deep innovation and specialized electronic security expertise.

40+

Countries with security technology capabilities and presence

- → 6 continents
- → #2 commercial electronic security company globally

1+ MILLION

Client sites worldwide

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

13,000+

Employees worldwide

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

Bringing Simplicity from Complexity for Businesses Around the Globe

With thousands of electronic security products, systems, and services to choose from, we help clients cut through the noise and see their needs clearly. Technology is advancing faster than ever before; our experts stay ahead of the latest innovations across intrusion, video, access control, fire detection, integrated systems, and more, so our clients can factor future technologies into their security roadmap.

A Trusted Advisor for Custom Integrated Security

Working hand in hand with businesses, we serve not only as their security technology provider, but as a trusted advisor and committed partner for a bespoke, personalized, and forward-looking client experience over the long term.

Connecting Clients to World-Leading Security Technology

Through our close partnerships with the world's foremost security technology innovators, technologists, and product manufacturers, we offer our clients unrivalled access to the most advanced and sustainable security solutions available today.

Driving Value from Business Security

We integrate seamlessly with each client's security team, providing end-to-end services across every aspect of security technology, from system design, installation, and integration to proactive monitoring, preventative maintenance, and intelligent remote services.

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

Securitas Technology

Our Approach to Innovation

Shaping the Future of Security Together

This report is just one result of a proven approach to security technology innovation refined over decades; an approach that has delivered some of the most advanced and complex security projects in the world and helped thousands of organizations of all sizes to continually optimize their security.

Client-Focused Activation

First and foremost, our innovation agenda is driven by close cooperation with our clients and a deep understanding of security across sectors and regions. Our **Security Symposiums**, **Client Advisory Board**, collaboration with the world's leading manufacturers and technologists, and active engagement across the industry inspire and inform our search for better technologies. Our **Client Engagement Centers** and **Technology Evaluation Labs** enable clients and prospective clients to see the latest technologies firsthand and gain insights on what technology is leading the industry.

Global Strategic Partnerships

We recognize that innovation in security technology is the result of an ecosystem of vendors across the globe pursuing new ideas and introducing new products. We are proud to partner with the world's leading providers of security hardware, software, analytics, and cloud infrastructure.

Robust Internal Evaluation

Our **Global Technology Strategy and Innovation team**, made up of security experts from around the world, is always looking ahead to meet our clients' future needs. They work closely with our business leaders and strategic partners to identify and evaluate the benefits of new technologies and to understand the proper applications for the different technologies. The team also assess new products to ensure they are technically sound and commercially viable, all to improve our range of solutions and services.

People and Process Excellence

Finally, we have developed expertise across functions and regions to deliver these innovations to our clients. Our capacity to design, install, monitor, maintain, and continually update integrated security technology has made us a trusted advisor for organizations large and small.

Our **Global Clients Program** is specialized to deliver these benefits even to the world's largest enterprises whose security needs span the globe.

Learn more about the Securitas Technology Global Clients Program

securitastechnology.com/global-clients-program

SecureStat® HQ™ Security Management Platform

Gain clarity and control over security operations to enable continuous improvement.

SecureStat® HQ™ is an all-in-one digital security management platform that simplifies security management, connects users to their security systems and Securitas Technology's services, and generates insights to optimize security and business performance.

Enterprise-Level Site Control

- Organize and see locations across the enterprise.
- Set site schedules to drive consistency.
- Edit contacts and call lists to keep sites up to date.

Efficient System Management

- Control multiple systems: access, video, fire, intrusion, etc.
- Manage user access across systems.
- Test systems from anywhere with internet access.

Real-Time Event Management

- Activity Messenger to see activity across locations.
- Alarm Messenger to see and respond to alarms.
- Service Messenger™ for service request updates.
- Installation Messenger to monitor installation projects (coming soon).

Direct Client Gateway

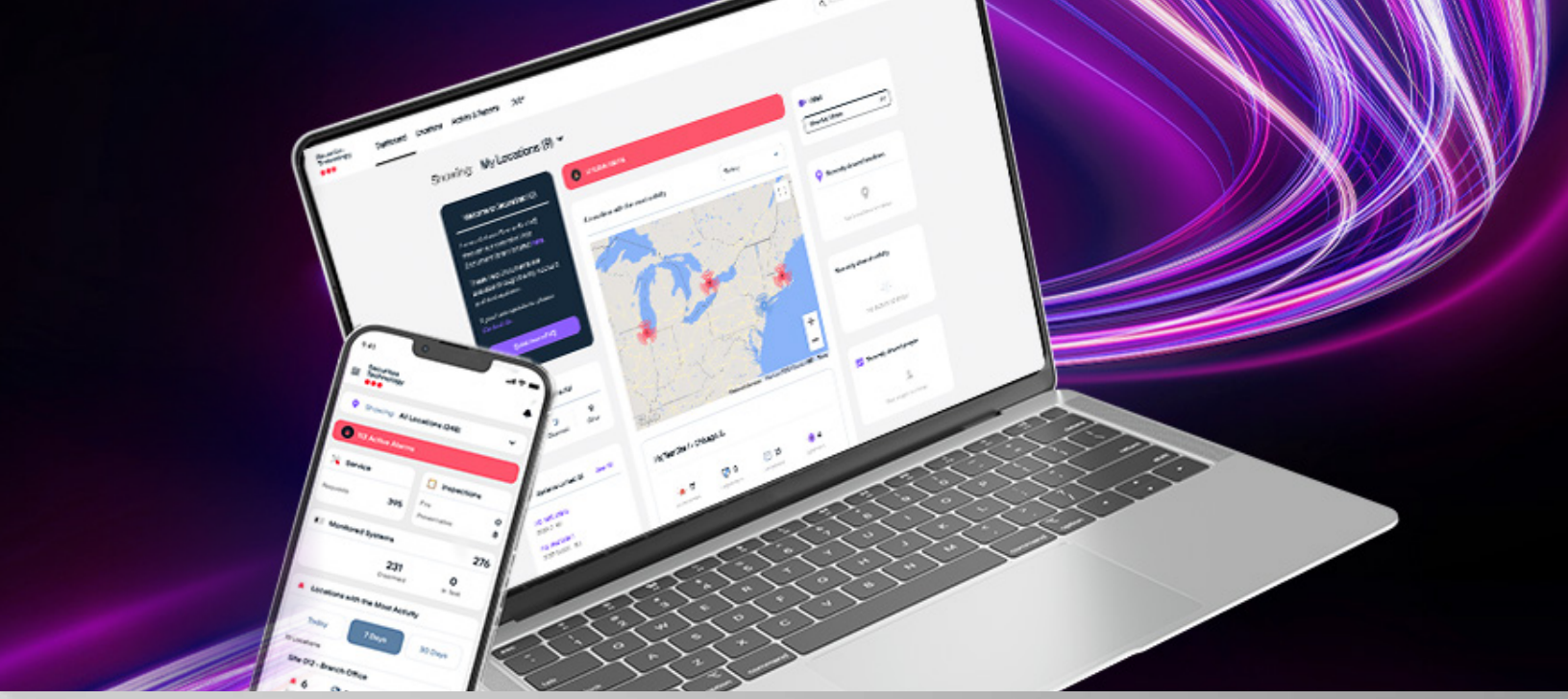
- Open service tickets and connect with Support.
- View and pay invoices.
- View live and recorded video.

Intelligent Data Insights

- Dynamic and customized reporting.
- Exception and event reporting.
- Report subscriptions to drive standardized reporting.

Simple Choice of Subscription Plans

- Basic, Advanced, and Premium plans available.
- Customizable to each organization's needs.
- Unlocks access to powerful advanced services delivered via SecureStat® HQ™, including SecureStat 360® Lifecycle Management.



Other SecureStat® HQ™ Features to Optimize Security Performance and Technology

SecureStat 360® Security Technology Lifecycle Management

Deliver greater security and organizational value through effective lifecycle management of security assets.

Maximize the life of equipment:
Know exactly when equipment was installed, its service history, and when replacement is recommended.

Cost-effective upgrade planning:
See what equipment needs replacement to plan upgrades efficiently and base investment decisions on data.

Reduce exposure to known vulnerabilities:
Easily monitor software and firmware versions and end-of-life status to proactively address outdated firmware or devices that are being sunset.

Document CO2e emissions:
View CO2e emissions per device from power consumption and make informed choices to align security investments with sustainability goals.

SecureStat® Video

See live video and recorded video associated with an event.

SecureStat® Access

Remotely manage access control systems.

SecureStat® Alarm

Remotely manage intrusion detection systems.

1 Executive Summary

On the Horizon for the Security Industry in 2026

The key trends, challenges, and opportunities facing security professionals in 2026 and beyond.

About the Report

Crafted for security professionals by security professionals, the 2026 Global Technology Outlook Report combines an exclusive set of data sources with deep industry expertise, extracting actionable insights into technologies, strategies, and innovations influencing the commercial security market now and in the future.

These sources of data and expertise include:

Market Survey: An external market survey commissioned by Securitas Technology, with 575 responses from verified security professionals in the United States, France, United Kingdom, Germany, Sweden, and Australia. The survey, served to electronic security technology decision makers and professionals with direct involvement in technology investments, focused on current technology utilization, future adoption, and planned investment.

2024 Client Survey & Advisory Board Feedback: A survey process managed by Securitas Technology with responses from over 4500 clients across 17 countries. The 2024 Global Client Survey included questions relating to planned security technology adoption and investments. Insights were also gathered from members of the Securitas Technology Client Advisory Board – a diverse group of clients that provide Securitas Technology with feedback on their security technology challenges and needs representing different industries.

Technology Partner Consultation Process: A consultative process managed by Securitas Technology to gather survey data and industry insights from 24 participating strategic technology partners. These partners include 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 & Innovation team, Global Technology Review Committee (GTRC), and Global Technology Innovation Council (GTIC).

2026 Outlook: What Security Professionals Are Seeing

Our 2025 report highlighted the growing importance of data in electronic security, and explored how it is changing the industry – creating new value but also requiring new expertise in cloud technology, artificial intelligence (AI), analytics, data privacy, and cyber hygiene.

These trends have accelerated in the last year. Across the globe, the explosive growth in AI model development and the use of AI in daily life is driving heavy investment into improving data connectivity and data center infrastructure.

While security technology has been taking advantage of cloud infrastructure, analytics, and AI for several years, we are now seeing security manufacturers and developers deepening the features of their products and solutions – across video, intrusion detection, access control, and more.

The outlook for 2026 sees the sustained prominence of three key security technology trends already having a transformative impact on the industry: **AI, Cloud Applications, and Advanced Sensors.**

Greater sophistication and availability of these technologies will lead to increased adoption, with greater focus on leveraging the data collected by security devices and applications to **drive value in other areas.**

Survey data featured in this report revealed that **enhanced employee safety** is the number one driver behind organizations' future security investments. In addition to this, the report dives deeper on several mounting business challenges that are set to be priorities for security professionals in 2026. These include:

- **Protecting people in increasingly volatile business environments**
- **Moving to real-time and proactive incident management strategies**
- **Driving value and organizational impact through security deployments**

These trends, the increasingly rapid pace of change in technology, and the threat environment require organizations to build continuous technology evaluation into their security programs. A phased approach to adopting new technologies, with support from an experienced partner, can help security professionals to plan effectively for integrating technology smoothly into their organization's security program.

What is certain is that standing still is not an option. Planning ahead now is the best insurance against having to play catch up in the future.

Key Takeaways

1

The AI landscape will evolve further driven by the development of generative AI (GenAI) use cases, such as natural language search, and increasing processing power. AI will help transform systems integration, combining data sets from disparate systems to produce composite security and business intelligence.

Read More: Section 2, page 22

2

Cloud-based technology is the new normal and will become the basis for many new security system implementations. Migration from on-premises infrastructure to cloud configurations will continue – first via a hybrid approach – as organizations pursue benefits such as centralized management and improved scalability.

Read More: Section 2, page 26

3

The integration of advanced sensors will expand thanks to increasing compatibility with security systems. By leveraging more data from sensors, organizations will seek to ensure compliance, improve efficiency, and enhance client and employee experiences.

Read More: Section 2, page 30

4

Increased global tension and volatility are major concerns for organizations. We're seeing the prioritization of technologies to help improve employee safety and crisis communications alongside strategies for improved risk intelligence, emergency preparedness, and disaster recovery.

Read More: Section 3, page 36

5

Reactive incident response is shifting to proactive threat detection. Integration of alarm management tools with multiple data sources and AI virtual agents will increase automation and accuracy, helping human agents to become more efficient and better anticipate threats.

Read More: Section 4, page 54

6

Organizations see the potential of security technology as value driver. From enhancing employee and customer experience to supporting sustainability goals, security technology is gaining respect in the boardroom as a tool to unlock efficiencies and help optimize business operations in a multitude of ways.

Read More: Section 5, page 72

Data Trends & Insights

Client Trends

We surveyed our clients in December 2024 on their current use of technology and plans for future technology adoption.

Most Adopted Technologies[1]

Percent saying they currently use:

[1]In-house branded survey of 4540 Securitas Technology clients in Australia, Belgium, Canada, Denmark, Finland, France, Germany, Ireland, Mexico, Netherlands, Norway, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States. Conducted November 2024.

Top Trending Technologies[1]

	Currently use:	Planning to adopt in the next 12-18 months:
1	29% Mobile Smartphone Credentials	30% Artificial Intelligence
2	28% Cloud-Based Solutions & Storage	27% Mobile Smartphone Credentials
3	26% Visitor Management	25% Visitor Management
4	11% Artificial Intelligence	24% Predictive Analytics
5	8% Touchless Biometrics	20% Touchless Biometrics
6	7% Predictive Analytics	20% Cloud-Based Solutions & Storage

Top Subscription Based Technologies[1]

	Currently use:	Planning to adopt in the next 12-18 months:
1	43% Managed & Hosted Access Control	27% Video Alarm Verification
2	43% Fire & Emergency Preparedness Training	20% Managed & Hosted Video
3	39% Managed & Hosted Video	16% Online Client Management Portals
4	37% Mobile Response Guarding	15% Fire & Emergency Preparedness Training
5	25% Video Alarm Verification	15% Managed & Hosted Access Control
6	24% Online Client Management Portals	11% Mobile Response Guarding

Data Trends & Insights

Market Trends

We conducted an in-depth survey of security and loss prevention professionals across multiple markets to identify the key trends and use cases in security technology.

Cloud Technology Adoption and Plans[2]

Cloud-based systems are now mainstream.

Cloud Adoption on the Rise

Use of cloud-based electronic security technology across organizations:

18% Are fully cloud based today

34% Expect to be fully cloud based in 5 years

Efficiency Gains Driving Cloud Adoption

Reasons for adopting cloud-based systems:

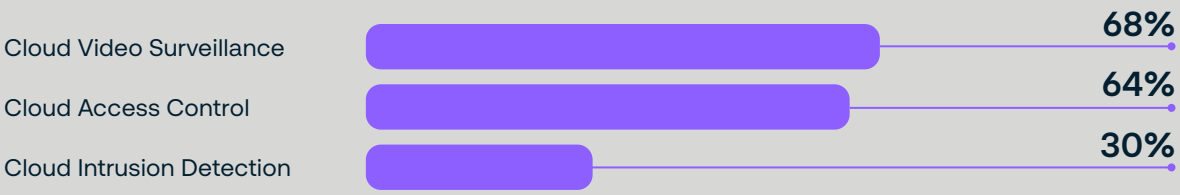
#1 – Centralised security management

#2 – Increased efficiencies

#3 – Easier to use and manage

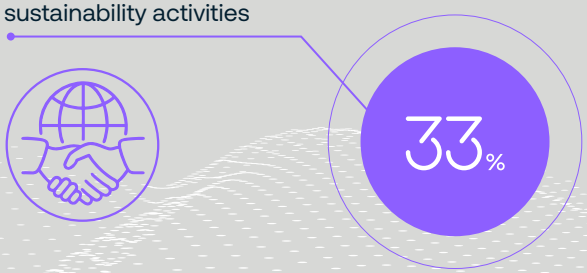
Top Cloud-Based Systems

System adoption by organizations using cloud solutions:

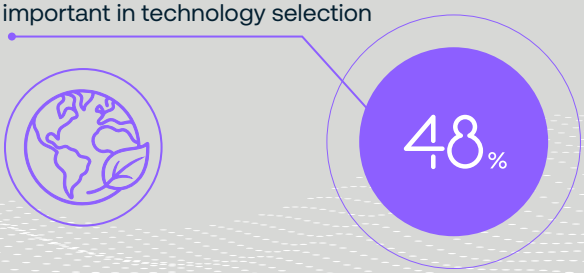


Involvement in Sustainability[2]

Participate directly in sustainability activities



Consider sustainability important or very important in technology selection



AI Adoption and Plans[2]

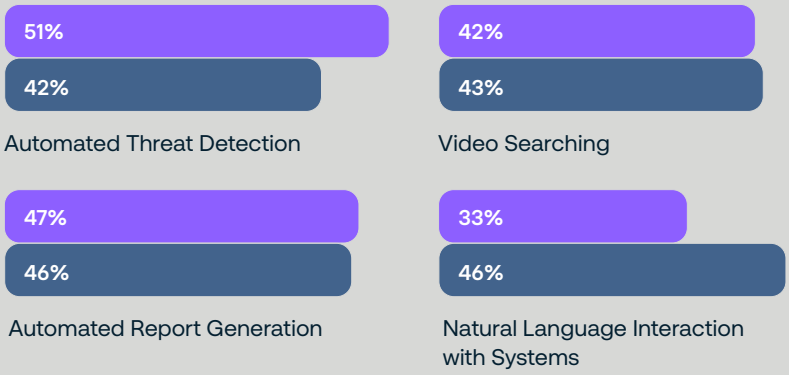
AI is an integral part of security technology, with strong interest in new use cases.

Top Current AI Use Cases

- 36% Object Recognition
- 35% Intrusion and Loitering Detection
- 27% People Counting
- 26% Anomaly Detection
- 24% Vehicle Detection, Speed, and Direction

Top Future GenAI Use Cases

● "Definitely" or
● "Somewhat" interested:



Advanced Sensor Technology Adoption and Plans[2]

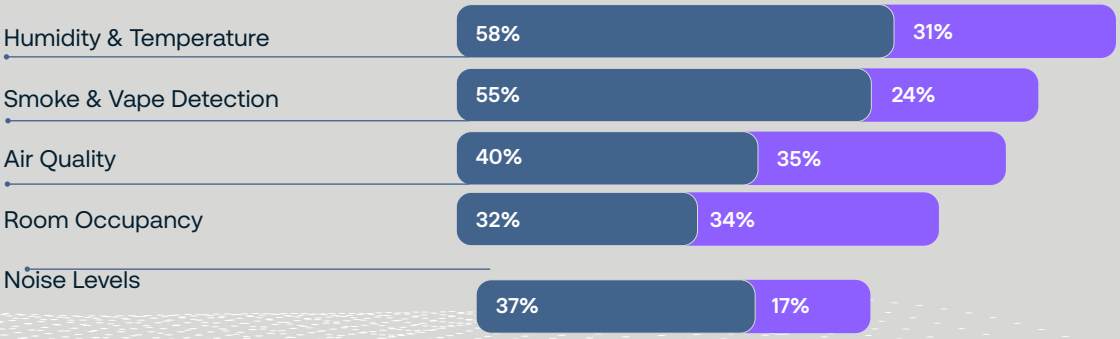
Advanced sensors are widely used as part of security, and most organizations are looking to expand further.

Advanced Sensor Adoption within Security

- 9% Extensively Using
- 39% Partially Using
- 35% Planning to Implement
- 16% Not Using

Top Advanced Sensor Use Cases

● Currently Use ● Plan to Use:



[2]Third-party blind survey of 575 security and loss prevention professionals with decision-making authority for security technology in Australia, France, Germany, Sweden, the United Kingdom, and the United States. Conducted February & March 2025.

Partner Insights

We surveyed our strategic technology partners for their insights on the direction of security technology and their innovation plans.

50%
Ranked AI as the top trend in the industry

Top 3 Security Technology Trends

1

AI Applications

"Everyone from the CSO and CEO level down is trying to identify how their organization can use AI to take advantage of the cameras they already have."

Hanwha Vision

"Agentics: AI agents as autonomous systems capable of understanding contexts, making decisions, and taking actions independently."

milestone

2

Cloud Technology

"There is a massive uptick in interest in Cloud solutions that enable the use of Generative AI models to search recorded video."

VERINT

"We expect that small and medium-sized businesses, as well as distributed enterprises, will be the quickest adopters."

MOTOROLA SOLUTIONS

3

System Integration

"Modernizing security systems also unlocks the value of centralization, aggregating various components into one platform."

brivo
simply better security

"New integrations on the market simplify the deployment of central station monitoring software, making a multi-site VMS installation more approachable."

EAGLE EYE NETWORKS

Steps to Supporting Sustainability

1

Product Design

"Sustainability guides our design process, ensuring longevity, efficiency, and recyclability that helps you reduce your carbon footprint."

resideo

"Our development toolkit focuses on eight areas, including raw materials, water, virgin material, end-of-life reusability, recyclability, in-life energy consumption, carbon footprint, and financial cost."

ASSA ABLOY
Opening Solutions

2

Equipment Power Consumption

"We are developing energy-efficient surveillance systems that reduce power consumption and carbon footprint."

MARCH networks
A Delta Group Company

"One key area is our support for hybrid and cloud-based architectures, which enable organizations to optimize their hardware footprint, reduce energy consumption, and scale more efficiently".

INTELLICENE
UNIFYING SECURITY. ENABLING ACTION

3

Operational Practices

"We have set goals to minimize water use in our manufacturing and only choose materials classified as safe—eliminating hazardous materials."

AXIS COMMUNICATIONS

"IDIS Americas is committed to supporting sustainability in security technology with long-lasting, durable products that minimize waste and reduce the need for frequent replacements."

IDIS One Solution. One Company.

Top Product Development Priorities

1

AI and Analytics Integration

"AI-driven analytics to provide real-time incident detection, anomaly recognition, and proactive threat mitigation."

MARCH networks
A Delta Group Company

"Using AI to improve user experience and speed and scale of operations."

VIAKOO

2

Cloud Solutions

"Cloud-based solutions to enable greater scalability, flexibility and remote management."

MOTOROLA SOLUTIONS

"Enterprise-grade cloud and mobility solutions."

Honeywell

3

Integration and Interoperability

"Modernizing security systems also unlocks the value of centralization, aggregating various components into one platform."

Software House C·CURE IQ

"More open API's into the DMP Ecosystem for greater compatibility into disparate systems."

DMP

4

User Experience and Interface Improvements

"Simplify event data visualization and analysis to help identify anomalies, see trends or patterns, and correlate events."

OpenEye

"Modular, purpose-built, mobile-friendly applications that solve customer problems."

AMAG TECHNOLOGY
An Allied Universal Company

5

Sustainability and Efficiency

"Strong emphasis on energy-efficient and environmentally friendly solutions."

SONITROL

"Sourcing more raw materials and components close to where they are produced… allows us to meet our goals of lower carbon emissions."

ASSA ABLOY
Opening Solutions

> "These insights from our industry-leading strategic partners come direct from the front line of global security innovation, offering our clients a technology developer's perspective on what's coming next."

Doug Walsh | Global VP, Technology Strategy
Securitas Technology

2

Technology Trends to Watch **in 2026**

The rapid pace of innovation in artificial intelligence (AI), cloud computing, and advanced sensors is having a profound impact on security technology – not only in the technologies themselves but in strategies for deployment, maintenance, and use.

Across the globe, the growing accessibility of these groundbreaking technologies is transforming the way we live, work, and progress into the future. For the security industry, the opportunities are vast. The world's leading manufacturers, software developers, and innovators are embracing these technologies to create new, enhanced features across video surveillance, intrusion detection, access control, and more.

For security professionals, this means increased integration, greater protection, and more efficient security management.

AI is Accelerating Everything

AI is today in widespread use, but its transformative capabilities continue to drive the global tech space. Substantial investment in unleashing AI's immense potential is enabling the rapid development of previously unimaginable capabilities that are not only keeping AI in the headlines but impacting virtually every sector of the economy and society.

AI is not new to security technology either. In fact, AI has been finding applications in security for some time, whether machine learning (ML) and data analytics in video surveillance and threat detection solutions or AI-powered use cases for license plate recognition, occupancy management, facial recognition, object detection, object tracking, and more.

These and other applications of AI will develop in sophistication and reach, and our market survey shows that AI is now seen as a core technology of the security space.

According to our market survey, 70% of organizations are already leveraging AI in their security program[1].

> AI and AI agents specifically are transforming the security industry with applications in access control, identity management, and security management platforms, by offering enhanced efficiency and data-driven decision-making.
>
> **HID**

A New Generation of AI Emerges

As we enter 2026, AI is now accelerating past the ML phase to enable greater automation and generation of insight. This is where Generative AI (GenAI) comes into play.

According to our market survey, the majority of organizations across markets are interested in GenAI use cases.

Recent research by McKinsey[2] also shows that GenAI is a very accessible technology, with most users in non-technical roles. That holds strong potential for the security industry.

One immediate application that delivers greater efficiency and security is anomaly (or exception) detection. This technology is moving from rules-based programming to deep learning, leveraging GenAI. In video surveillance, GenAI algorithms can be deployed to understand a "normal" scene and identify specific variances that give context to what's happening in real time – for example, a person wearing dark clothing entering a restricted area. These algorithms can be fine-tuned offline by human agents and then redeployed to one or multiple cameras with edge capabilities. A similar evolution is occurring with audio detection. The ability to detect abnormal audio has been around for a few years; what is now possible is for AI virtual agents to identify what the abnormality is – a car, a piece of equipment, etc. – giving human agents immediately actionable information.

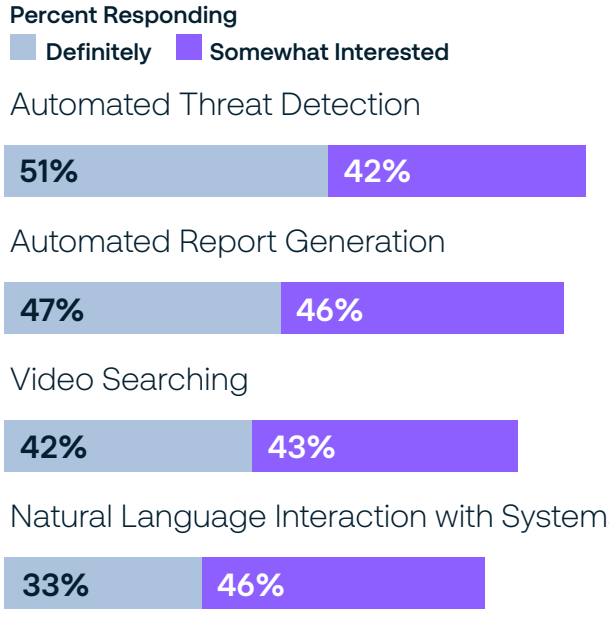
AI's Impact Across Security Applications

Even established security use cases are being enhanced by AI. For example, facial recognition technology for biometric access control has been around for many years, yet AI improves the accuracy and reliability of authentication by continually observing and learning changes in people's appearance.

The same effect is being seen within integrated security management. AI's ability to integrate and analyze data from multiple sources makes it possible to recognize trends or patterns in the data that could highlight a potential issue. As a general example, AI may suggest that false alarms occur more often on a certain day of the week, at a certain time of day. Or, in the retail environment, identifying unusual point-of-sale transactions occurring while a particular employee is on shift. These examples provide security managers with real data to address a variety of challenges, from managing false alarms to preventing internal theft.

While AI is unlocking new and exciting opportunities for security professionals – and will certainly increase in importance over time – every organization should carefully choose AI use cases when looking for ways to enhance security and business value. It will also be important to be aware of the evolving ethical and regulatory requirements linked to AI.

Organizations Are Ready for GenAI[1]



[1]Third-party blind survey of 575 security professionals with decision-making authority for security technology in Australia, France, Germany, Sweden, the United Kingdom, and the United States. Conducted February & March 2025.

[2]"The human side of generative AI: Creating a path to productivity." McKinsey Quarterly, March 18, 2024. https://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/the-human-side-of-generative-ai-creating-a-path-to-productivity

Partner Insight

Getting Smarter About AI

It's hardly a bold statement to predict that AI will continue to reshape security and surveillance. AI technology is already a vital element of many organizations' surveillance roadmaps. Combining AI with on-board audio and video analytics is enabling highly accurate object detection and classification with fewer false alarms – plus helping customers receive actionable data that can drive intelligent monitoring, enhance operational efficiency, and generate data-driven business insights.

But now that AI has moved well past being an emerging technology, the question our industry needs to ask is, "How do we use AI in new ways to go beyond security and impact the future direction of our organization?"

The question our industry needs to ask is, "How do we use AI in new ways to go beyond security and impact the future direction of our organization?"

We'll continue to see open platforms and generative AI models emerge, supporting more granular capabilities such as the ability to "talk" to a device and say, "Detect the man with the red shirt between 1:00 and 2:00 am on the lobby camera." Also, the video market is probably growing stronger than other security category. One significant factor is the advancement of AI technology, which is causing manufacturers to rethink their roadmap for AI inclusion in most of their product lines.

Our industry has to come together and create guidelines and benchmark standards around AI, determining what level of accuracy is generally acceptable for most security and surveillance applications. It is good for everyone – end users, dealers, and manufacturers – to be held to a standard. We have specifications and standards for cameras. There's no reason not to have a standard for AI accuracy.

The combination of AI and intelligent analytics allows security professionals to design and build safer and more efficient surveillance environments, especially as comprehensive, AI-powered intelligent technologies continue to evolve into total business solutions.

Partner Insight

Honeywell

AI Applications in Access Control

Several verticals are leading the adoption of AI-enabled security and safety systems, in response to industry-specific needs and technological advancements. Healthcare, retail, manufacturing, and data centers are among the industries we are seeing the fastest integration of AI solutions for security.

For example, hospitals and medical facilities use AI-powered security system to improve patient safety and better monitor facility access. AI-enabled predictive maintenance and security monitoring systems are being utilized in data centers, as well as electronic access controls, biometrics, and AI-powered security cameras to help maintain security around the physical facility.

We have seen greater sophistication in AI-powered solutions to enhance security monitoring and incident response. In our recent survey*, security and occupant safety is one of the top use cases of how AI is being deployed in buildings today.

More than 60% are deploying AI to monitor for unusual behavior, more than half are using it for location tracking, and 45% cited use of biometrics-based access control systems.

In addition, AI can be used to aggregate and mine data from many different sources such as access events, visual events, and alarms.

AI use case adoption by organizations for building security*

Unusual behavior →	**60%+**
Location tracking →	**50%+**
Biometrics-based access control →	**45%**

AI can then be used to find non-obvious relationships which can predict where there may be security vulnerabilities so that security professionals can be more proactive and pre-emptive.

In this way, AI is helping security teams stay ahead of the ever-changing threat landscape. In a similar way, system vulnerabilities can be detected and mitigated to avoid disruptions through automated patch management.

Honeywell commissioned Wakefield Research to conduct the Honeywell Building Managers Research Survey, which polled 250 U.S. building managers and senior decision makers across building types including offices, hospitals, airports, schools, universities, hotels and data centers. To participate in the research, respondents had to use AI-enabled property management systems in buildings with 250+ occupants.

*mckinsey.com/capabilities/people-and-organizational-performance/our-insights/the-human-side-of-generative-ai-creating-a-path-to-productivity

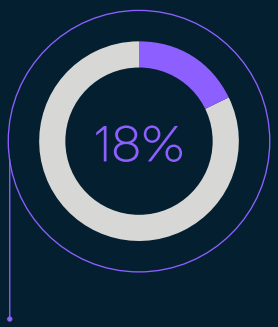
Cloud Applications as the New Normal

The electronic security industry has realized strong benefits over recent years from the rapid rise of cloud-based solutions: scalability, simpler implementation, and easier maintenance and cyber hygiene. The global growth of data center infrastructure also means that solutions are now widely applicable to organizations of all kinds, and for many different security use cases.

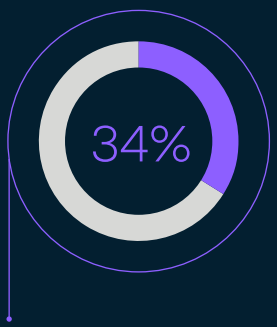
We can say with certainty that cloud-based security technology is fully mature, and it is now part of many organizations' future plans. **According to our market survey, 18% of organizations are already fully cloud-based[1].**

Cloud Adoption Continues to Rise[1]

Use of cloud-based electronic security technology across organizations:



Are fully cloud-based today



Expect to be fully cloud-based in 5 years

[1]Third-party blind survey of 575 security professionals with decision-making authority for security technology in Australia, France, Germany, Sweden, the United Kingdom, and the United States. Conducted February & March 2025.

Demand is Driving Data & Cost Efficiency

True enterprise-level cloud solutions are here, and our strategic technology partners are making major investments in their cloud data infrastructure, matching the sophistication of other technology sectors. This means even organizations that manage security technology at a global level can leverage cloud as their default for physical security applications, with a private cloud as an option.

In addition, more and more security applications are now available on the cloud: video surveillance, access control, intrusion, and others.

As demand for data increases alongside cloud investment, the cost of bandwidth for data storage and processing is beginning to fall. In parallel, this is paving the way for innovation in areas such as video surveillance, which is one of the most data-hungry technologies. Camera manufacturers are focusing on improved video compression algorithms. By significantly reducing video bitrate and storage costs, these developments will help accelerate the adoption of cloud-hosted and AI-powered video platforms.

Hybrid Cloud: A Solid Stepping Stone

As cloud solutions become mainstream, a hybrid approach offers a stepping stone for organizations on their journey to fully-cloud-based security technology. Such organizations can progressively expand their cloud-based systems while continuing to use on-premises systems through the end of their lifecycle or because some applications and environments call for it.

However, we do see increasing awareness among organizations of the burden of maintenance and regulatory compliance that comes with running on-premises infrastructure. When these costs are fully included, the total cost of ownership for cloud solutions becomes much more attractive.

> “Cloud technology allows organizations to manage security remotely, scale their infrastructure as needed, and integrate multiple security functions into a single platform.”
>
> 3xLOGIC

Our market survey reveals that the critical factors driving cloud adoption are the ease of maintenance, centralized management, reduced operating costs, and increased efficiency. These are compelling benefits that are hard to ignore.

For late adopters, the good news is there is a robust body of best practice for cloud solutions to help ensure data security, proper protection of personally identifiable information (PII), and system resiliency. As is the case here at Securitas Technology, security integrators will play an important role in helping organizations to create a clear plan for adopting cloud-based technology, with every business needing to consider their own, unique requirements to achieve a smooth transition.

While some organizations will choose to stay with on-premises technology, and many will take the hybrid path, the trend line is clear. Cloud technologies will be fundamental to the future evolution of security.

Partner Insight

The Path to Cloud-Based Security Systems

Organizations are rapidly moving systems to the cloud for good reason. Cloud-based security technologies offer remote access and management, allowing businesses to monitor and control facilities from anywhere.

Scaling and connecting new technologies are simpler with cloud-native solutions, and businesses can reduce expenses related to on-site servers, maintenance, and IT support, freeing teams to focus on core business priorities instead of system maintenance.

Despite the clear advantages, migration concerns still remain a barrier for many organizations. They worry about their existing hardware investments—what happens to on-premises control panels and downstream devices? Products like the Brivo Mercury Solution address these concerns by easily and affordably transitioning existing Mercury control panels to work in the cloud, with minimal disruption along the way.

> Hybrid VMS solutions are designed with built-in cybersecurity measures, ensuring compliance, resilience, and data protection.

This approach eliminates the need for costly “rip-and-replace” upgrades while still delivering cloud benefits and a modern security system.

Modernizing security systems also unlocks the value of centralization, aggregating various components into one platform. For example, a unified security platform, like Brivo Security Suite, brings access control, video intelligence, visitor management, and intrusion detection into a single dashboard.

A centralized cloud-based platform serves as a single destination for all security needs, providing that coveted “single pane of glass” view across every location. This reduces the need to juggle multiple security platforms and tools, while reinforcing cybersecurity. And, with cloud-based security, you gain access to real-time security metrics and information that’s woven and connected into your business systems for faster, more informed business decisions.

Partner Insight

The Future of Video Surveillance: Hybrid VMS Unlocks Scalability and Flexibility

In today's rapidly evolving technological landscape, businesses seek surveillance solutions that offer scalability and flexibility.

Hybrid Video Management Systems (VMS) represent an advancement in video surveillance, combining the best cloud and on-premises deployments to meet diverse needs.

Hybrid VMS solutions, like the combination of **Milestone's XProtect and Arcules**, provide unparalleled scalability by leveraging cloud infrastructure. This allows businesses to expand their video surveillance capabilities seamlessly, accommodating increased data storage and processing requirements as organizations grow.

Flexibility is another advantage. Businesses can tailor their surveillance to specific needs with various cloud deployment options, including pure cloud, edge cloud, and camera to cloud, integrating them with on-premises systems. Hybrid VMS offers the freedom to adapt and evolve, whether robust security or cloud agility is required.

Moreover, hybrid VMS solutions are designed with built-in cybersecurity measures, ensuring compliance, resilience, and data protection. This secure-by-design approach provides peace of mind, safeguarding video data against potential threats.

Integrating cloud and on-premises systems also enhances business intelligence. Harness video data, coupled with advanced analytics and AI from Arcules, and make faster, more informed decisions, improving security and operational efficiency. This future-proofing capability ensures surveillance systems remain relevant and effective in the face of changing demands.

In conclusion, hybrid VMS scalability and flexibility revolutionize the video surveillance industry. Solutions like Milestone's XProtect and Arcules pave the way for an adaptable and resilient future by offering deployment freedom, robust security, and enhanced business intelligence.

Advanced Sensor Applications Are Evolving

The potential for advanced sensors and other connected devices (sometimes referred to as the Internet of Things or IoT) has been a much-hyped topic within the security industry for many years. And indeed, discrete devices for detecting flooding, temperature and light conditions, air quality, sound, smoking, and vaping are well established.

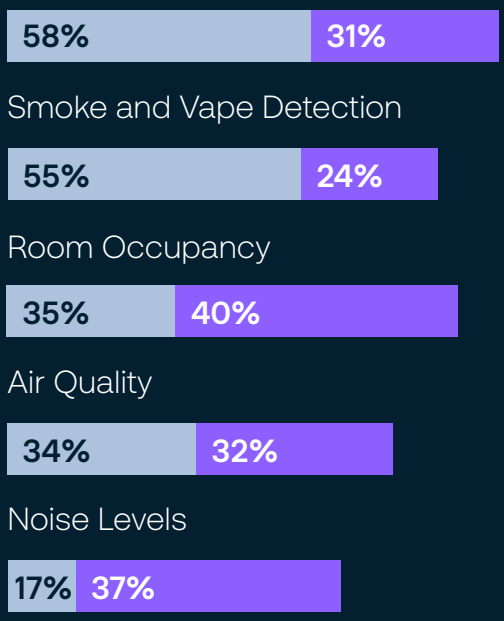
Our survey reveals that 61% of organizations have integrated advanced sensors with their security systems[1].

However, the industry has struggled to deliver value beyond the direct application of simply sending an alert to enhance security or operational efficiency. Now, that is starting to change.

Monitoring for More[1]

Percent Responding

Currently Use **Plan to Use**



[1]Third-party blind survey of 575 security professionals with decision-making authority for security technology in Australia, France, Germany, Sweden, the United Kingdom, and the United States. Conducted February & March 2025.

Surveillance Cameras Transforming into Multi-Sensors

Thanks to advances in AI and data analytics, many forms of environmental monitoring can now be proactively achieved without a separate sensor device. Innovation in video surveillance technology offers a great example of this. Cameras that leverage AI capabilities – either built into the device ("on the edge") or connected to video analytics software – are being used as multi-sensor devices.

By monitoring a scene over time, AI algorithms can help identify anomalies; not only security threats, but also unexpected environmental changes, such as smoke, fire, animals, crowds, and even gunshots. Using video systems as intelligent multi-sensors can help automate response by delivering precise information to a human agent.

Unlocking Business Value Through Sensor Integration

Security and environmental monitoring aren't limited to managing external threats. There is also value to be unlocked by leveraging data captured by integrating sensors with security systems to help optimize health, safety, and business operations.

In the retail sector, security and environmental sensors can combine to reveal key insights into customer behavior, from tracking room occupancy data to mapping customer footfall; valuable data that can support future marketing efforts.

Our market survey also found that over a third (37%) of organizations plan to leverage sensors to monitor noise levels[1]. This application is relevant in many sectors where noise can have a negative impact on employees and customers.

In manufacturing, for example, sensors can help protect workers against excessive noise from industrial machinery. Manufacturing is also a strong candidate for humidity and temperature monitoring – provided by environmental sensors, thermal cameras, and video analytics – to help provide production supervisors with early warnings of overheating machinery.

Compatibility vs Cybersecurity

Increasing compatibility is set to continue driving the integration of sensors into electronic security platforms – a trend that will allow organizations to create more widely connected ecosystems for monitoring their business environment.

However, when considering which environmental or other connected sensors to integrate with private security networks, organizations should work in close partnership with their security technology provider to evaluate product vendors and ensure their devices meet the required standards for quality, support, and cybersecurity.

Partner Insight

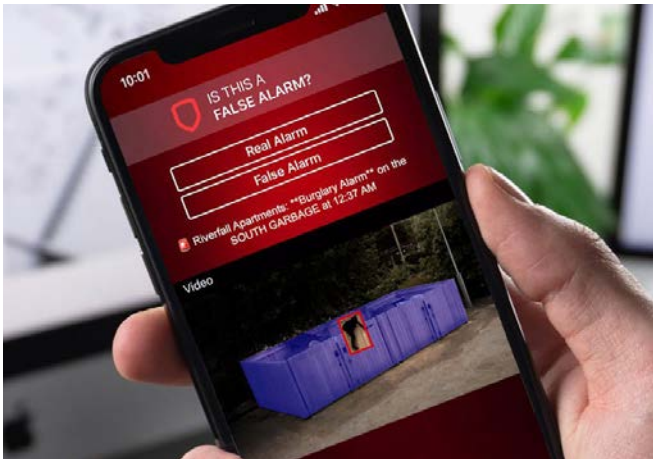
Turn Cameras into Powerful Alarm Detection Devices

The rapid maturation of analytics software makes it possible to bring advanced analytics to existing video surveillance cameras.

Solutions such as **DMP's XV Gateways** with AlarmVision® turn standard IP cameras into powerful alarm detection devices. By enhancing motion detection with analytics and seamlessly integrating video events with intrusion alarm panels, organizations can stay on top of events with instant notifications.

Reduce False Alarms

Direct communication between camera and intrusion panels turns cameras into intelligent motion detectors able to trigger actions and alarms. Through video analysis of the event, the subject of the motion is determined before sending the alarm, empowering end users to verify videos and enhancing monitoring center video verification.



Beam Replacement

Installing beams for detection not only takes time and resources, but the solution also itself is often unreliable and prone to triggering costly false alarms. Security systems with cameras in tandem can not only effectively replace detection beams, but far exceed their capabilities. By integrating cameras with the intrusion system control panel, cameras turn into powerful alarm detection devices with specific zones; in the case of AlarmVision, up to four zones can be customized for each camera.

Seasonal Flexibility

Yet another benefit is the flexibility to accommodate seasonal activities and changing needs. Rather than having to visit the site and hire additional labor to move beams or wires, camera zones can be quickly and easily adjusted. Seasonal shifts in activity and inventory may be complicated, but advanced solutions like AlarmVision can greatly simplify protection.

Partner Insight

resideo

Connected Security Sensors: Revolutionizing the Security Landscape

In an era where smart technology is transforming every facet of our lives, security systems are no exception. Resideo is advancing the security industry with its ProSeries connected security sensors. These innovative devices are reshaping how homeowners, businesses, and security professionals approach safety and security.

Resideo's ProSeries sensors integrate cutting-edge technology to communicate seamlessly with the main panel and mobile devices. This connectivity enhances the performance of the sensors, delivers real-time updates and remote capabilities while providing users with an unprecedented level of control over their security systems.

Connectivity enhances the performance of sensors, delivers real-time updates, remote capabilities while providing users with an unprecedented level of control over their security systems.

The sensors include a range of options, each equipped with advanced features such as enhanced encryption, superior false alarm reduction and OTA updates. These sensors can be easily connected to other smart devices, creating a fully integrated ecosystem. Whether it's a home or business owner receiving an alert at work or monitoring their property from afar, Resideo's connected technology allows for a more proactive and responsive approach.

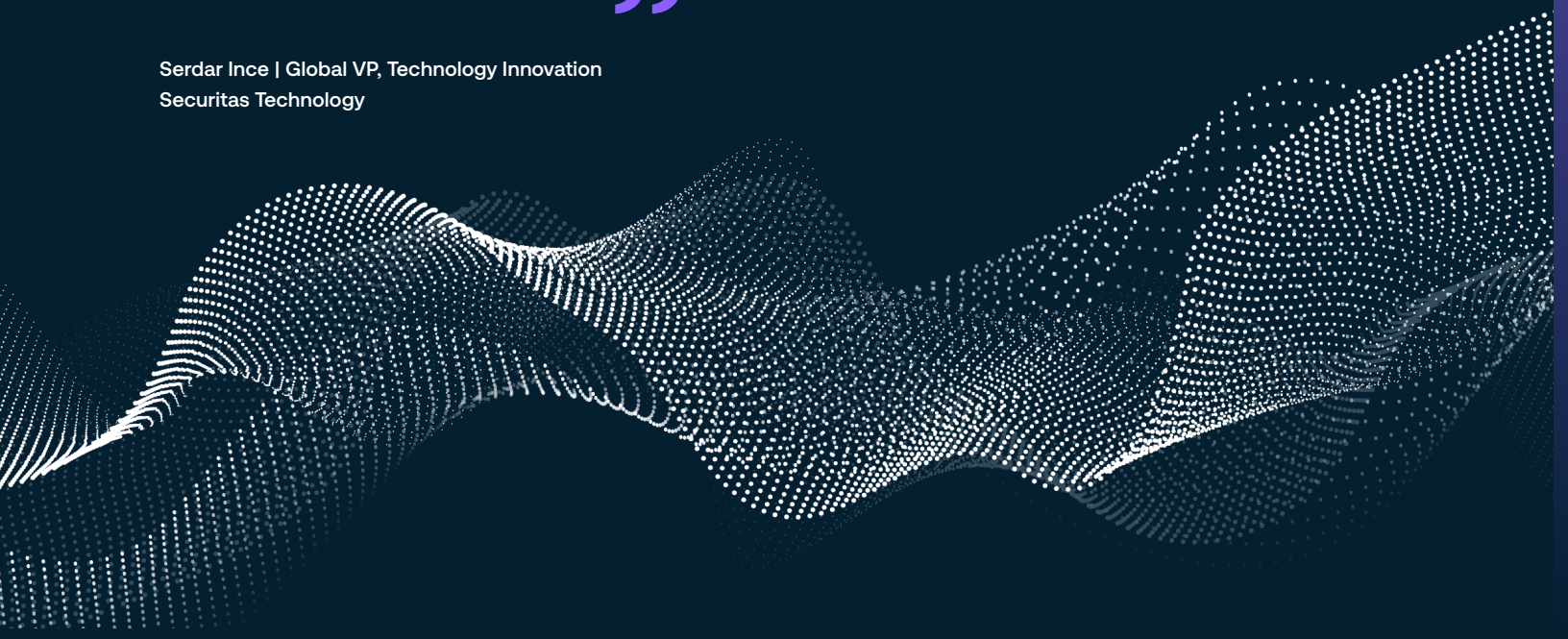
Moreover, the system's use of cloud-based technology allows for easier management and troubleshooting, reducing downtime and improving system reliability. The continuous advancements in wireless communication and data encryption also ensure that the ProSeries sensors are not only efficient but secure.

By embracing the Internet of Things (IoT) and providing flexible, scalable solutions, Resideo is pushing the boundaries of what's possible in security. The ProSeries connected sensors are a major leap forward, making security systems smarter, more user-friendly, and better equipped to handle the evolving needs of today's world.

Action Plan for Security Professionals

> GenAI is set to transform video analysis. It will enable clients to extract detailed context and generate instant insights. When we pair this with cloud technology, we can process and manage everything more efficiently. And with the increasing compatibility of advanced sensors, we can extend security further through a connected ecosystem driving business efficiency and intelligence.

Serdar Ince | Global VP, Technology Innovation
Securitas Technology



Artificial Intelligence

1

Define an AI Data Strategy

Identify the data sources and security challenges or opportunities that AI can help address. Specific examples may include object detection and tracking, vehicle recognition, or anomaly detection. Setting clear objectives will help ensure the use of AI is purposeful and aligned with the organization's overall security strategy.

2

Understand Regulatory, Legal, and Ethical Requirements

Seek legal team guidance to ensure AI applications comply with regulations and data privacy laws. Consider the ethical implications and establish a governance process for responsible use. This will help build trust and safeguard information. A formal, multi-functional AI review committee may help organizations develop clear and compliant AI guidelines and ensure that they are properly implemented.

Cloud Applications

3

Build a Cloud Migration Model and Roadmap

Develop and implement a clear migration model and roadmap with defined milestones and timelines for transitioning security operations to the cloud. Leverage a security technology provider to help identify the right combination of cloud-based solutions and services for future security needs.

4

Partner with Specialist IT Teams

Work together with the IT department to leverage their specialized knowledge and co-create a plan for implementing a cloud-based security technology model. This will include identifying infrastructure requirements, considering cybersecurity risks, and implementing cyber hygiene processes.

Advanced Sensors

5

Establish Sensing Needs

Identify the specific sensor applications and environmental conditions that support security and business goals, such as regulatory compliance, improved efficiency, or employee and client experience. Then, work with a security technology partner to determine the best approach for integrating advanced sensors with the existing security technology infrastructure.

6

Validate Vendors & Device Compatibility

Thoroughly assess potential vendors and technologies to confirm they meet the necessary standards for quality, compliance, and cybersecurity. Evaluate aspects such as end-point security, known vulnerabilities, and data storage practices to help ensure robust protection and seamless integration.

3 Security Solutions for a Volatile Environment

Society and security professionals have been responding to an uptick in volatility ever since the upheavals of the COVID-19 pandemic period.

Today, this trend shows no signs of slowing; if anything, volatility fueled by geopolitical tension, economic uncertainty, and extreme weather is increasing in many parts of the world. Security professionals need to prepare for a range of low-probability but high-impact events, from workplace incidents to social unrest to natural disasters.

It's a topic of concern for our Client Advisory Board too, who told us that keeping their people, premises, and assets safe in the face of increasingly unpredictable business environments has become progressively more challenging.

Technology Improving Safety in All Environments

A number of new technologies are helping organizations improve safety for all – whether that's workers in the office or remote locations, clients and customers in a bank or store, or children in a school. Here, we explore innovative ways organizations are ensuring they stay prepared for any eventuality.

Employee safety is the top investment driver[1]

A majority of respondents in our survey cited employee safety as a top 3 driver of security technology investment

with **30%** ranking it first.

Monitoring for More Risks

Helped by advances in AI, cloud applications, and advanced sensors, security professionals are discovering more ways to monitor their organization's working environment for a multitude of safety and security risks. These include:

- **Protecting beyond the perimeter:** Technologies such as Light Detection and Ranging (LiDAR) integrated with existing perimeter intrusion detection systems provides pre-emptive, real-time, and high accuracy detection across large areas – whether the external site boundary or an internal facility, such as a warehouse.
- **Responding to suspicious sounds:** Audio analytics built into multi-sensor devices or AI-driven video surveillance systems help not only detect sounds but also classify them, enhancing situational awareness and response capabilities. For instance, a video system equipped with audio analytics can be taught to filter out everyday sounds, such as traffic, but immediately alert to critical sounds like gunshots or human distress calls like "help!"
- **Sensing environmental conditions:** Integrating environmental sensors with electronic security systems is helping organizations identify and respond to more threats or conditions such as distinct changes in the environment. Examples include unauthorized smoking and vaping, the presence of harmful chemicals in the air, sudden and unexpected temperature shifts, the sound of aggressive behavior, and more.

[1]Third-party blind survey of 575 security professionals with decision-making authority for security technology in Australia, France, Germany, Sweden, the United Kingdom, and the United States. Conducted February & March 2025.

Managing Emergencies Efficiently

A critical aspect of every organization's security program, effective incident management can be the difference between minor disruption and major disaster. Organizations are turning to technology applications to improve how emergencies and incidents are handled in the moment:

- **Mass Notification Systems:** Common in schools and campus environments, this technology provides fast and effective incident communications, allowing security professionals to alert large audiences to security and safety risks, such as natural disasters or an active shooter, in real time. Instant notifications delivered through mobile devices, voice messages, and other digital channels help guide people to safety with updates on situational status, emergency protocols, evacuation instructions, and lockdown scenarios. **Mass notification to mobile devices was a top 5 technology for future adoption in our market survey, identified by 22% of respondents**[1].

- **Information Sharing with Emergency Responders:** In North America, it's becoming increasingly common for high-risk organizations to share security and safety surveillance footage directly with first responders. By providing access to feeds from one or more high priority cameras – via the cloud – organizations can empower responding authorities with enhanced situational awareness, helping them to respond more effectively in the event of a call to emergency services.

Remote Services for Uninterrupted Security

Finally, we're seeing more organizations investing in remotely managed services to ensure their security systems are optimized, secure, and performing effectively. Key examples of these services include:

- **Preventative System Health Monitoring:** An always-on, managed service designed to optimize the health and performance of security systems. It combines AI tools and professional human agents to proactively detect potential issues, such as battery failures or camera view interference, and reduce system downtime.

- **Firmware and Password Management:** These automated, remote services help organizations to keep security systems connected to their IT network updated and protected against external cybersecurity threats.

- **Protecting Operations Remotely:** Remote services have become essential for protecting business operations, especially during natural disasters or crisis events that restrict physical access to buildings. When access is not possible, remote services can help monitor and secure the premises. They help protect against issues like loitering and looting, which can be common after natural disasters such as hurricanes.

> "Security products now use AI, sensors, and analytics to identify threats early. Integrated systems combine cameras, access control, alarms, and intercoms to verify and act quickly. The result is reduced delay between detection and response = minimized impact."
>
> **Resideo**

Partner Insight

Technology Strategies for Business Continuity

Physical access control systems are crucial to the safety and security of everyone who require access to a customer's facilities. To keep these systems running and resilient, it is imperative that Business Continuity Planning is considered during system design and continually managed during the life of a system.

Network Design Considerations

Embedded, network access controllers are stand-alone by design – if the network fails, the controller continues to make access decisions and buffer access events. But during the failure, events and alarms are not transmitted up to system operators. To improve resiliency, controllers should have both a primary and backup network port, routed through different network paths to the system head end (on-premises or in the cloud). If the primary network fails, the second port takes over and continues to route traffic, ensuring that alarms get delivered.

For on-premise systems, the head end must also be considered. Make sure to provide a High Availability (HA) setup with two servers or VMs that provide complete backup operation. Even better, locate the backup server in a different but close location to provide instant failover. For the ultimate in resilience, design in a Disaster Recovery (DR) server that provides a "warm" failover in case the HA setup fails.

For cloud-based systems, choose a provider that offers multiple availability zones to guard against failure of a single location. And make sure that the backup strategy for the system database is sound – periodic backup / restoral points every hour as a minimum.

Zero-trust networking is a great way to increase the reliability and resilience of your network design, especially for cloud-based systems. This may require additional network devices, but the result is a system more resistant to cyberattacks.

Operational Considerations

Business continuity is improved by following rigorous cyber hygiene to mitigate vulnerabilities before they affect your system. Maintain a rigorous software update process for both controllers and head end software and conduct periodic penetration tests to discover and mitigate vulnerabilities.

Another important action is to proactively monitor system operation, predict possible failures, and alert on these conditions. Is the system's hard drive reaching capacity? Is network traffic showing high latency or retries? Are you getting database errors? Sometimes even small indicators are a sign of something more ominous.

Finally, don't forget your batteries! Seriously – monitor and change backup batteries for access controllers to keep controllers humming during AC power loss.

Partner Insight

Increasing Workplace Security with Digital-First Access Management

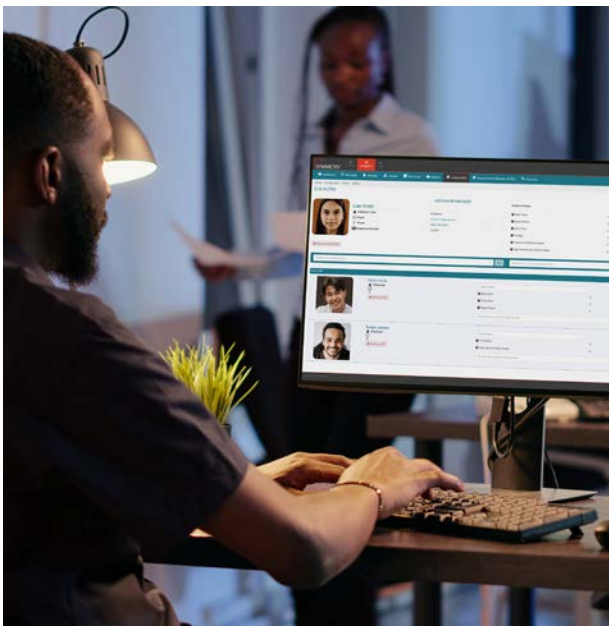
As workplace security threats evolve, organizations must modernize their access management strategies to protect people, assets, and data effectively.

A digital-first approach to access management strengthens security, improves efficiency, and provides real-time intelligence to mitigate risks proactively.

Digital-first access management leverages mobile credentials, intelligent automation, and analytics to provide a seamless and secure experience. Employees and visitors can use their smartphones to access facilities, reducing reliance on physical badges and minimizing security risks associated with lost or stolen credentials. Additionally, security teams can remotely manage permissions and monitor access attempts in real time, ensuring a rapid response to potential threats.

Another advantage of digital access management is its ability to integrate with identity management solutions, such as **AMAG's Symmetry CONNECT.** By linking access control to HR and IT systems, organizations can enforce security policies automatically, ensuring only authorized personnel can enter specific areas.

Organizations must adopt a proactive approach to workplace protection. Digital-first access management offers the agility, intelligence, and efficiency needed to safeguard workplaces from evolving threats. By embracing these advanced technologies, businesses can enhance security while improving operational efficiency, ensuring a safer and more resilient workplace for the future.



VERINT

Partner Insight

Fraud Prevention: Lessons for Other Industries from Banking

In today's rapidly evolving landscape, security is a critical pillar of operational integrity and customer trust.

Handling vast amounts of sensitive data, banks need a comprehensive security approach to tackle both cyber and physical threats. The convergence of IT and physical security teams is vital for survival in this competitive market.

Banks have learned that traditional security strategies – where IT and physical security teams operate separately – are no longer effective. Modern technologies like biometric access control and AI-powered video surveillance require integrated oversight. Cloud-based solutions further blur the lines between physical and digital security, underscoring the need for collaboration.

Aligned teams can better address complex threats like ATM skimming and digital account takeovers. Integrated strategies combining anti-skimming technologies with enhanced surveillance and real-time data sharing help prevent fraud before it occurs.

Effective fraud prevention also relies on human awareness. Insider threats are significant, and banks implement programs and training to ensure employees can identify and respond to insider risks.

Leadership plays a key role in fostering a unified approach, advocating for measures that combine technology with adaptable strategies. Those strategies must be flexible to address unique operational and regulatory requirements. Regular training should cover new technologies and specific challenges faced by the organization.

Consideration must also be given to the internal situation. Internal expertise is highly valuable and establishing security hubs can help tailor strategies to meet specific needs. Internal threats should not be overlooked. Security programs must balance protection with employee privacy, fostering trust within the organization.

The integration of IT and physical security teams is essential for successful bank security, offering lessons for other industries: eliminate silos, promote collaboration, and emphasize continuous training. Banks that have successfully unified their security operations offer valuable insights for organizations looking to safeguard assets, maintain customer trust, and remain resilient in the face of evolving risks.


Securitas
Technology
Securitas
Technology

Strategies to Prepare Organizations & People

Beyond implementing cutting-edge technologies, organizations are increasingly investing in advanced threat anticipation strategies. Leveraging up-front intelligence and conducting thorough post-incident analysis, security professionals aim to stay better prepared for – and protected against – future security events.

Intelligence-Led Security

In today's interconnected world, volatility, uncertainty, complexity, and ambiguity (VUCA) are ever-present challenges. Because of this, we're seeing a growing market for commercial risk intelligence services that are enabling organizations to stay a step ahead of risks.

In our survey, there was strong interest in risk intelligence, **with 20% (tied for top spot) saying that they are planning to integrate such services into their security program**[1].

Risk intelligence services are helping security professionals decide where to focus their security investment, leveraging information to establish which of their locations are at greater risk. They help bring a proactive approach to risk through features such as:

- **Risk Forecast Reports:** Offering organizations crucial situational awareness updates, delivered on a daily, weekly, and monthly basis. These reports are tailored to provide insights at local, national, and global levels, helping organizations stay informed and prepared for potential risks.
- **Crime Index Reports:** Delivering cutting-edge crime analysis, from global and national trends, right down to the neighborhood level. This technology-driven service helps organizations to see, compare, study, and forecast crime data in the areas they do business using interactive maps, detailed statistics, and AI-powered analysis.

Preparation Is the Key to Enhanced Safety

From natural disasters to fire to workplace violence, organizations face a multitude of potential safety risks that can rapidly escalate into an emergency. Preparation is vital when it comes to cultivating calm, compliant, and confident responses to crisis situations.

Interest in emergency preparedness services is increasing, with more organizations realizing the importance of proactive planning to protect the safety of people and the workplace.

According to our market survey, **88% of organizations have implemented a formal plan for response to emergency situations**, showing that this is an area of focus for security professionals[1].

However, **18% also say that they have low or no confidence in their preparedness**, so this must remain a priority for organizations[1].

These services offer organizations support in several ways, from planning and compliance to employee training:

- **Emergency Planning:** Creating customized Emergency Action Plans (EAPs) and Fire Prevention Plans (FPPs) to document how an organization responds to emergency situations and measures to prevent incidents from occurring in the first place.
- **Compliance Services:** Ensuring an organization's emergency planning procedures are documented, updated, and meet the requirements of relevant regulatory bodies.
- **Training Services:** Education for employees on how to deal with varying safety and emergency situations through in-person and virtual training. Topics include fire safety, active shooter response, first aid training, counter terrorism, and more.

AI-Assisted Security Planning & Procedures

AI is transforming organizational security by enabling the extraction of critical information from security systems using simple text or voice commands. "Conversational AI," utilizing Natural Language Processing (NLP) and Natural Language Understanding (NLU), has the potential to streamline post-incident investigations, carry out routine security checks, and even prepare systems for high-priority events.

For example, systems can be pre-set with specific protocols in preparation for a known high-priority event. Imagine an important client is visiting the head office, requiring heightened security. Relevant security system could be given the simple command to "raise the security level" without requiring any further action by the security team. This proactive approach not only enhances security but also builds stakeholder confidence by demonstrating a commitment to safety and preparedness.

88%

Of organizations have an emergency response plan[1]

Confidence in their plan:

Very confident **9%**
Confident **39%**
Moderately confident **35%**
Slightly confident **16%**
Not confident at all **2%**

[1]Third-party blind survey of 575 security professionals with decision-making authority for security technology in Australia, France, Germany, Sweden, the United Kingdom, and the United States. Conducted February & March 2025.

Partner Insight

Genetec™

The Power of Cloud Storage

The need for additional storage increases over the lifetime of your VMS. Your video retention policies evolve, and you may need to introduce redundant archiving and other mechanisms to protect your data.

In many cases, adding on-premises storage comes with significant hardware and installation costs. As an alternative, you can opt for hybrid or full-cloud storage. You gain the ability to change your storage capacity without purchasing additional hardware and add layers of retention and redundancy. This helps you comply with policies and regulations while protecting your data against disasters and cyberattacks with triplicate copies saved in the cloud.

With a modern software-as-a-service (SaaS) solution, cloud storage capabilities are built-in. You can connect devices straight to the cloud, making it easier to scale your operations with minimal to no additional requirements for on-premises infrastructure.

[Cloud storage] helps you comply with policies and regulations while protecting your data against disasters and cyberattacks.

Genetec™ Security Center SaaS offers cloud-native capabilities, with direct-to-cloud camera support, continuous cloud recording and playback, and fully hosted video operations. With hybrid capabilities, there are also options to push recording and processing to the edge, connect to on-premises infrastructure, and many more deployment options to fit your unique requirements.

Work with your channel partner to find the best video management solutions, architecture, and deployment options. There are many ways to store video and metadata locally and in the cloud. A hybrid approach can maximize flexibility at every site. Your integrator can help optimize your system and operations to make the most out of your investment in physical security.

Partner Insight

VIAKOO

Safeguarding CPS from Cybersecurity Risks

The proliferation of powerful IoT systems (also known as Cyber-Physical Systems, or CPS) from smart sensors to AI cameras, offers efficiency but significantly expands the cyber-attack surface.

Effective exposure management is the only way to address new (and old) cyber threats. Enhanced physical security hardware with neural processors, advanced networking, and custom memory creates a "hacker's playground." Neural processors enable local, sophisticated attacks and botnet participation. Faster networking facilitates quicker data exfiltration and malware spread. Custom memory stores sensitive data locally, becoming a prime target.

Real-world implications include increased DDoS attacks, data breaches exposing critical information, supply chain vulnerabilities, manipulation of physical security systems, and espionage.

Real-world implications include increased DDoS attacks, data breaches exposing critical information, supply chain vulnerabilities, manipulation of physical security systems, and espionage.

Protecting businesses requires strong cyber hygiene and automation. The scale and heterogenous nature of physical security deployments means you need to use automated methods. Key practices include automated firmware updating, network segmentation to isolate CPS devices, device hardening by disabling unnecessary services, strong passwords frequently changed, implementing a zero-trust architecture, thorough supply chain security assessments, and employee education on CPS security.

The rise of powerful CPS devices presents both opportunities and risks. Understanding these risks and implementing robust security measures is crucial for businesses to harness the power of CPS while minimizing cyberattack exposure.

Preparation is no longer optional; it's essential. Viakoo helps businesses discover and remediate CPS vulnerabilities and is proud to work with Securitas Technology in leading the charge on addressing the challenge of physical security cyber threats approaching at AI speed.

Partner Insight

INTELLICENE
UNIFYING SECURITY, ENABLING ACTION

Security to Scale

As businesses scale and expand into new locations, they welcome the opportunity for growth but also face an increasing set of security challenges. Managing security across a larger footprint can quickly become a complex and overwhelming task—one where disparate systems, siloed data, and a lack of centralized oversight can leave critical vulnerabilities exposed.

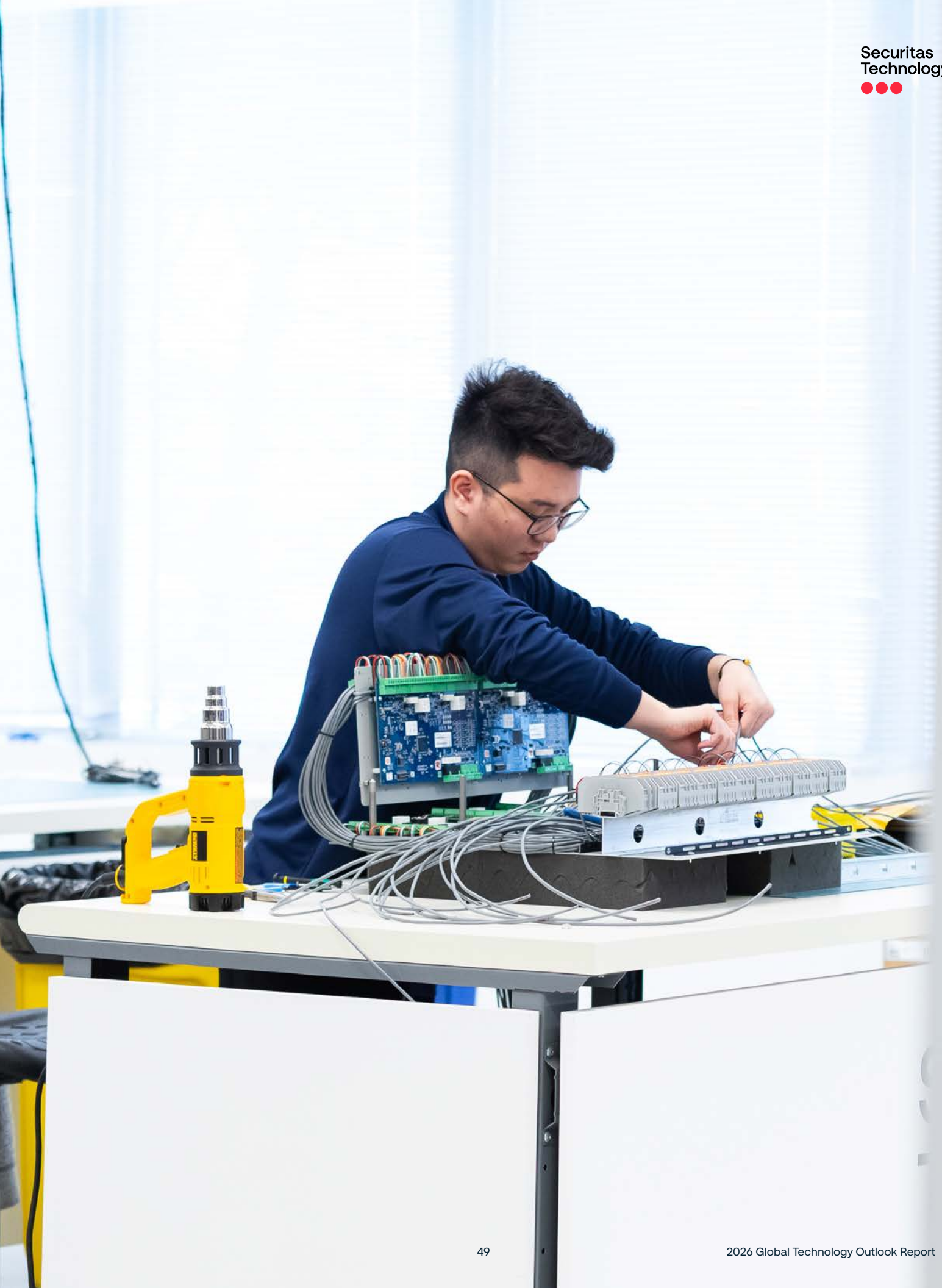
Having a security system that's built to scale is key. Rather than having new locations manage their security portfolio in their own separate lanes, centralized security management platforms can empower security teams to get a comprehensive view of each site's security posture with centralized, correlated data streams and boundless potential for integrations.

> Enterprises can convert correlated security data into actionable insights to improve operations.

By unifying disparate security systems into one centralized platform, security personnel can unlock the holistic visibility they need to identify, assess, and prevent emerging threats from escalating into full-blown incidents. Beyond just security, enterprises can convert correlated security data into actionable insights to improve operations by tracking customer activity patterns and employee productivity to determine where resources are best spent and maximize efficiency.

Enterprises need a security portfolio capable of changing and growing with them. Scalability and flexibility aren't optional – they're essential for maximizing security investments and ensuring long-term success.

Is your security strategy built to grow with your business?



The Future of Crime Risk Intelligence

Innovative Approaches to Safeguarding People and Places

Understanding the ebb and flow of crime is crucial for organizations to protect their stakeholders, particularly in regions where violence and crime trends can directly impact the safety of employees and operations.

The Importance of Crime Risk Scores

Crime risk scores, such as those by the Pinkerton Crime Index (PCI), provide an accurate, timely, and quantifiable measure of crime risk. Risk scores remove the uncertainty in gauging crime trends, helping organizations make data-driven decisions for strategic security planning, facility locations, resource allocation, insurance and liability, stakeholder safety, and reputation management.

Pinkerton Crime Index stands at the forefront of crime risk analysis, employing next-gen statistical machinery and innovative methods to capture the nuances of crime data.

Innovation and Technology Behind PCI

PCI stands at the forefront of crime risk analysis, employing next-gen statistical machinery and innovative methods to capture the nuances of crime data. The process begins with the meticulous collection of crime data from key sources including national, regional, and local law enforcement, and cross-referenced to establish a more realistic portrait of crime.

The data is then cleaned to address inconsistencies and underreporting. For example, accurate crime rates require correct crime counts/total offenses (numerator) and realistic population figures/crime per capita (denominator), reflecting the "floating population" or true number of people in an area — such as tourism and commuting behaviors — not just the residential population.

Accurate crime rates also carry a weighted severity reflecting their impact, gauged by factors like prison sentences and victim costs, ensuring more serious offenses have a greater influence on the overall risk score.

In the final step, forecasting algorithms undergo rigorous competition to hone their predictive accuracy.

Unique Challenges and Specialized Solutions

What makes PCI different from other crime forecasting solutions is in the way we approach the data — tailored unique challenges each country faces in crime data collection. PCI is currently for the U.S., Canada, Mexico, Brazil, the U.K., Sweden, and Australia.

For example, in Mexico underreporting is significant. Australian crime data varies vastly in publication timing and classification, leading to inconsistencies, while Brazilian reports show gaps in years and variances from local to national figures.

While many crime and risk products rely on baseline official reporting, PCI goes above and beyond — assessing additional data to fill the gaps missing from official reportage, such as victimization surveys, death certificates, and local expertise.

Above and Beyond

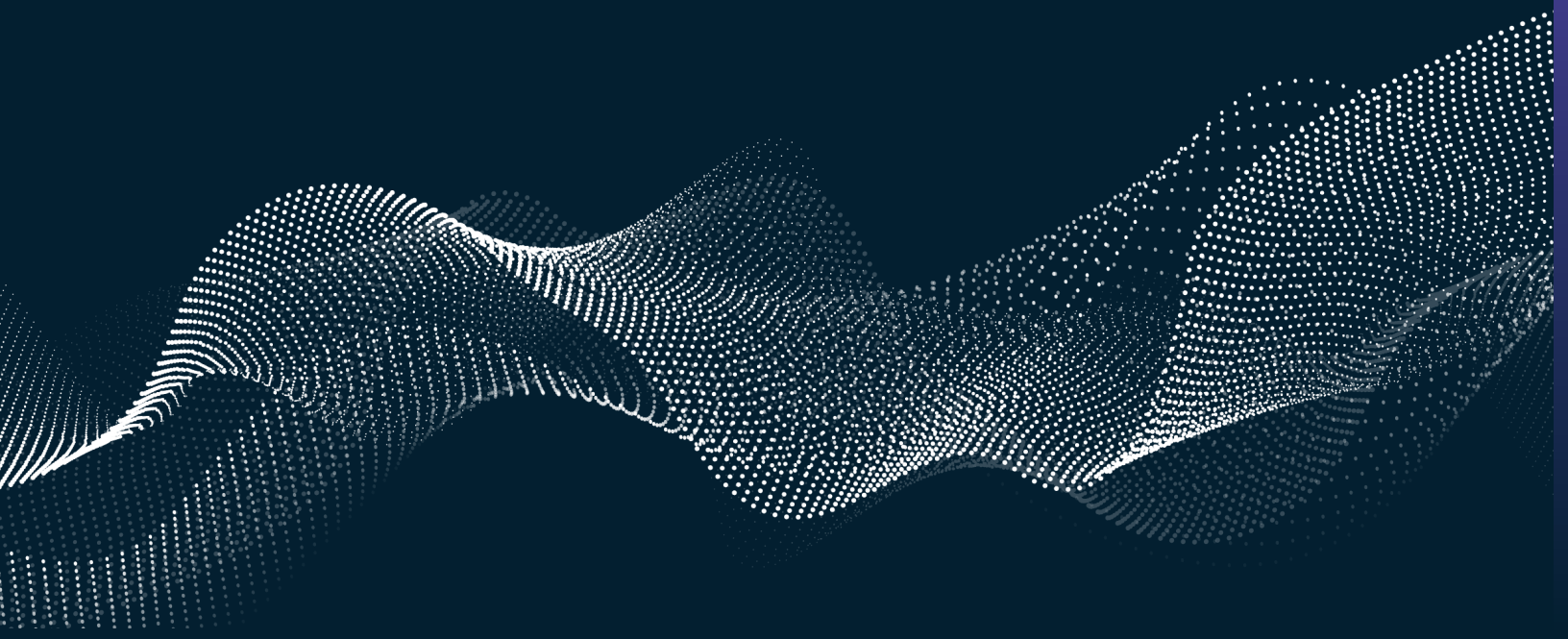
Updated monthly, PCI is not just a tool but a testament to the convergence of innovative data science and seasoned risk management, standing as a reliable, forward-looking crime risk tool.

Learn more at pinkerton.com

Action Plan for Security Professionals

> In today's volatile environment, enhancing security across all environments – from retail locations to campuses to corporate facilities – can be realized through advanced technologies like AI-driven analytics, emergency communication systems, and proactive incident management strategies.

Serdar Ince | Global VP, Technology Innovation
Securitas Technology



1 Review Technologies Used for Risk Mitigation

Evaluate existing risk mitigation and management approaches to identify areas for improvement. Consider new security technologies, training opportunities, and incident response strategies that can help enhance the safety of employees, clients, and the overall working environment.

2 Assess How to Stay Ahead of Risk

Review current processes and technologies for monitoring risk, and options to increase accuracy and speed. This could include investing in intelligence services to proactively identify potential threats so that the organization stays informed and prepared as new risks emerge.

3 Update Emergency Preparedness and Disaster Recovery Strategies

Continuously review and enhance business continuity and emergency preparedness plans. Focus on integrating technologies and communication strategies to improve response procedures, maintain operations, protect data, and ensure the safety of employees during crises.

4

Security Moving to Real-Time & Proactive Management

There is a major transformation underway in how organizations respond to events, whether through their own security team or a professional security monitoring provider.

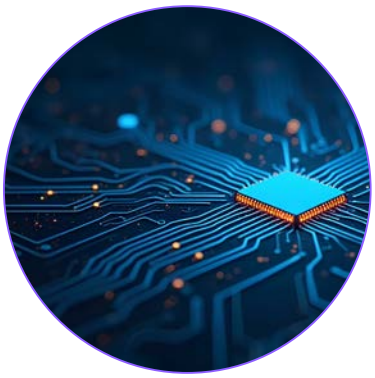
We are moving past the era of verification into one where AI-driven analysis of multiple data sources accelerates incident response and supports real-time decision-making – a security infrastructure that is continually learning and improving.

Looking further into the future, this data will be combined with other data sources to drive business intelligence relating to security, operations, and customer and employee experience.

Augmenting the Agent with AI

In the fast-paced world of security, the key to effective incident response lies in swiftly understanding what truly matters. As threats evolve, so must the methods of addressing them.

AI-driven technologies are revolutionizing the way human agents operate by providing them with precise information, allowing them to focus on complex problem-solving tasks. AI's strengths lie in its consistency and focus. Unlike human agents, AI never tires or gets distracted, making it an ideal virtual partner in the division of labor. This collaboration allows human agents to concentrate on what they do best: tackling intricate problems that require nuanced understanding and decision-making.



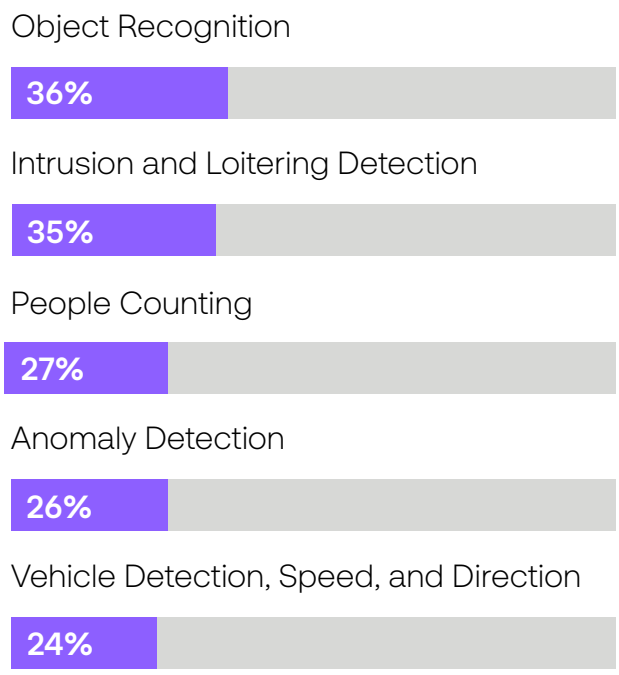
AI & Human Synergy Brings Advantages

One of the most significant advancements in this area is the dual analysis of video images. Equipped with edge analytics, cameras can now flag activities that may require a response. This initial analysis is then reviewed at the Security Operations Center (SOC), ensuring that potential threats are identified accurately. Every time a human agent spots an error, the AI virtual agent learns and improves, becoming more adept at distinguishing between benign and suspicious activities.

Virtual agents are also transforming alarm response by handling interactions with users during the verification stage. This capability not only makes alarm response more effective but also enhances agent productivity. By automating routine tasks, AI frees human agents to focus on more critical aspects of security management.

AI Already in Use for Automated Detection[1]

Percentage of organizations using:



Incident Response Becoming Increasingly Intelligent

Looking ahead, the sophistication of AI in incident response is set to increase. AI will soon be able to interpret complex situations with greater accuracy. Simple prompts in natural language, such as “Generate an alarm if someone is carrying a large package,” can lead to detailed and precise responses from virtual agents. This ability to understand and act on specific threats will be invaluable in environments like warehouses, where security needs are unique and varied.

However, as organizations embrace AI, they must remain vigilant about laws and regulations concerning privacy and the ethical use of AI. These considerations are crucial to ensuring that AI applications are both effective and responsible.

Ultimately, augmenting human agents with AI is not just about enhancing efficiency; it’s about creating a relationship where both human and machine excel in their respective roles. As AI continues to evolve, it promises to redefine incident response, making it more precise, proactive, and powerful. By leveraging AI’s strengths, security teams can ensure they are always one step ahead in safeguarding their environments.

[1]Third-party blind survey of 575 security professionals with decision-making authority for security technology in Australia, France, Germany, Sweden, the United Kingdom, and the United States. Conducted February & March 2025.

Partner Insight

EAGLE EYE NETWORKS

How AI Turns Security from Reactive to Proactive

Most footage that security cameras capture is never watched; there's simply not enough time. To make all this video useful, always-on AI can analyze video as it's captured to generate metadata, flag events, and automate responses. AI reduces response times, so people can focus on the incidents that matter.

AI provides real-world paths to proactive security:

Alerts based on designated triggers

Did a vehicle just pull up to the loading dock? Is there movement in a hallway after hours?

Eliminating expensive false positives

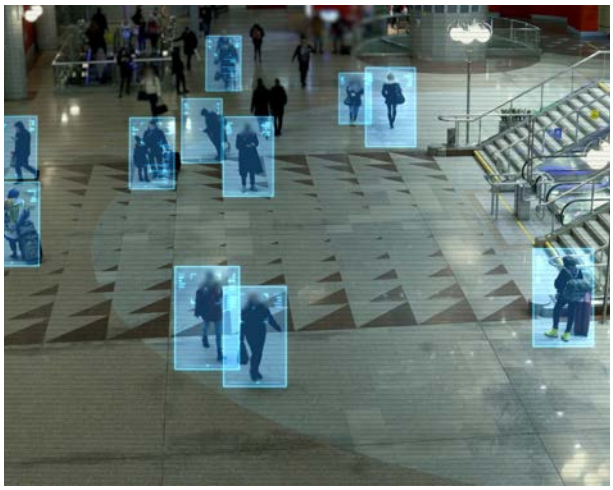
AI can nearly eliminate false alarms caused by weather or animals, avoiding expensive fines and making alarms more trustworthy.

Focusing search with AI

AI object recognition and tagging simplifies investigations with natural-language search terms like "person with backpack" or "red pickup."

Zooming in on vehicles and guns

Identifying vehicles is central to security incident investigation. **Eagle Eye's License Plate Recognition** can trigger alerts whenever a suspect vehicle appears on camera. And new gun detection technology can spot a weapon before it's fired.



AI that turns video into useful information can trigger incident alerts, spotlighting events for instant reaction.

Perhaps most importantly, the AI that turns video into useful information can also trigger incident alerts, spotlighting events for instant reaction.

The **Eagle Eye Cloud VMS** puts continual analysis and triage into practice — and provides a framework for extending its intelligence through an open API, already leveraged by a wide range of technology partners to deliver specialized software.

Partner Insight

Effective Alarm Verification Strategies

Traditional alarm monitoring follows a "Detect and Notify" model—when an alarm is triggered by a sensor, such as a motion sensor, a central monitoring station is notified. However, these alarms do not confirm an actual threat, leading to a 98% false alarm rate.

In response, many municipalities have introduced false alarm fines and/or require alarm verification before police dispatch. Some require alarm verification and provide priority police response to verified alarms that indicate a crime in progress.

To address false alarms, verification techniques like Multi-Trip Detection & Enhanced Call Verification reduce uncertainty but do not confirm a crime in progress. The most effective verification solutions are audio and video alarm verification, which allows central station operators to see or hear an incident in real-time, improving response times and accuracy.

> Some [municipalities] require alarm verification and provide priority police response to verified alarms that indicate a crime in progress.

Audio Verification

- Detects threatening sounds when the system is armed.
- Operators can listen in real-time to assess threats.
- Covers the entire space from floor to ceiling, wall to wall, enabling early alarm detection.

Video Verification

- Triggered by an alarm sensor or camera motion detection.
- Operators receive pre/post-alarm video clips or live video feeds.
- Provides visual confirmation of a crime in progress.

Integrating audio and video verification enhances alarm monitoring by reducing false alarms and improving police response. Audio provides full-space coverage and early detection, while video offers visual confirmation within the camera's view. Together, they maximize security and improve police response times and effectiveness, making them the gold standard for alarm monitoring today.

Partner Insight

BOSCH
Invented for life

Empowering Proactive Responses and Automated Decisions

AI is reshaping the role of video security with visual intelligence – helping users find meaningful information in video footage, recognize patterns, and understand what may happen next. Early, accurate detections make it easier to identify and respond to potential risks before they become a problem. AI-enabled solutions quickly and reliably detect perimeter breaches, brandished guns, missing personal protective equipment, and more.

By extraction, AI solutions and services can also aggregate and visualize data from multiple cameras for gathering insights on security, safety, and operations. Harnessing this data delivers information for trend analysis: by understanding patterns around situations that impact security or safety, users can make informed decisions that minimize the occurrence or impact of these events.

Recognizing and identifying patterns allows for alerts when situations need attention, empowering users to be proactive rather than reacting after an incident.

AI capabilities will soon expand beyond object detection for deeper scene understanding by interpreting complex environments and providing insights about what is happening. It will analyze images for situations without being trained for specific objects or behaviors. With integration into organizational processes, it can suggest actions to mitigate risk and alert personnel – bringing greater value to users.

AI capabilities will soon expand beyond object detection for deeper scene understanding.

Mining Data for Continuous Improvement

In the realm of security operations, the ability to monitor a broad array of data sources is transforming the landscape, offering new services that enhance both security and business intelligence.

New Tools Helping SOCs Work Smarter for Clients

Security Operations Centers (SOCs) are expanding their capabilities beyond system monitoring, paving the way for more sophisticated approaches to security and operations management.

Many additional services are already in place, such as asset tracking, which allows for real-time monitoring of an organization's vehicles and high value assets. With live access to a vehicle's location, the SOC can monitor the vehicle's journey and alert a logistics manager to any unexpected delays or safety incidents, ensuring smooth operations and heightened security. This kind of data integration exemplifies the potential of modern security systems to support business processes efficiently.

AI is also revolutionizing monitoring center operations, driving efficiency and effectiveness. Virtual agents can conduct tours of multiple cameras, identifying misaligned or out-of-focus cameras by comparing their installation state with the current state. This proactive approach ensures that surveillance systems are functioning optimally. Additionally, AI facilitates automatic remote maintenance, checking battery status, detector and door contact states, and ensuring images are stored correctly. These capabilities reduce downtime and enhance the reliability of security systems.

The Move to Predictive Platforms is Underway

Perhaps even more impactful is AI's ability to analyze event data to discern patterns, enabling organizations to better prepare for similar situations in the future. Many SOCs (including those of Securitas Technology) maintain a comprehensive data lake of alarm events, which can be analyzed for patterns, such as the time of day, day of the week, or seasonal trends. Organizations can also connect this information with other data sources for additional insight and to form a fuller picture of the total risk environment: operational and financial data, building automation system data, cyber threat monitoring, and more.

Predictive platforms based on this data are beginning to emerge, and within a few years, predictive analysis is likely to become a reality. We anticipate the development of new kinds of intelligence, such as event correlation, which will enable organizations to understand the factors that lead to incidents and anticipate when similar conditions might recur. This foreknowledge will empower businesses to take proactive measures, reducing risks and enhancing overall security.

In conclusion, the mining of data for continuous improvement is not just about reacting to incidents; it's about moving towards a predictive model that offers foresight and strategic advantage. As AI and data analytics continue to evolve, they promise to redefine security operations, making them more intelligent, responsive, and effective. By harnessing the power of data, organizations can ensure they are prepared for whatever challenges lie ahead.

> "AI capabilities do more than improve security outcomes; they also lower total cost of ownership by reducing the manual workload and allowing organizations to better utilize existing resources. From predictive threat analysis to automated responses, AI influences every aspect of our security solutions, helping clients stay ahead of evolving risks and making their operations more efficient."
>
> Software House

MOTOROLA SOLUTIONS

Partner Insight

Unlocking the Potential of Connected Security

The evolution of security demands a paradigm shift: from numerous disparate systems to a truly connected ecosystem.

For users, this isn't merely about device integration; it's about architecting an intelligent, adaptive security framework that anticipates and mitigates threats in real-time.

A cornerstone of this vision is open, interoperable platforms. By championing standards like ONVIF, we transcend vendor silos, fostering a dynamic ecosystem where best-of-breed technologies converge. This empowers organizations to tailor security solutions to their unique needs, driving innovation and resilience.

Furthermore, data-driven intelligence is paramount. We must harness the power of centralized analytics and AI to transform raw data into actionable insights. This enables proactive threat detection, automated responses and predictive security modeling, elevating security from a reactive to a preemptive posture.

In an interconnected world, cybersecurity becomes a strategic imperative. We must embed robust security protocols at every layer, from device authentication to network segmentation.

Cloud-based platforms facilitate remote management, real-time collaboration, and seamless data sharing, enabling organizations to respond swiftly to emerging threats and optimize operational efficiency.

A proactive, layered approach is essential to safeguard against evolving cyber threats and maintain the integrity of the ecosystem.

The strategic deployment of cloud technologies unlocks unprecedented scalability and accessibility. Cloud-based platforms facilitate remote management, real-time collaboration, and seamless data sharing, enabling organizations to respond swiftly to emerging threats and optimize operational efficiency.

Ultimately, a truly connected security ecosystem must be human-centric. We must design intuitive interfaces and provide comprehensive training to empower security professionals to leverage the full potential of these technologies. This fusion of human expertise and technological innovation is the key to unlocking a new era of security excellence.

By embracing these strategic imperatives, we can build a connected security ecosystem that not only safeguards assets but also drives operational efficiency and fosters a culture of proactive security.

Partner Insight

MARCH networks
A Delta Group Company

Enterprise Video Management for Multi-Site Locations

Managing video surveillance across multiple locations is challenging. Today's businesses need a system that centralizes video management, ensures system health, and delivers actionable insights to enhance security and operations.

March Networks' industry-leading enterprise video management solutions are designed to simplify management, offering scalable solutions for complex, multi-site deployments.

A robust video management system (VMS) enables businesses to monitor all locations from a single interface, simplifying day-to-day administration by offering centralized control via desktop, web, or mobile. With **March Networks Command Enterprise Software** (CES), organizations can monitor and manage thousands of cameras, recorders, and video channels, with real-time system health monitoring, user activity tracking, and customizable views to keep security teams proactive and responsive. Managing and updating devices across multiple locations is easy, with bulk firmware upgrades, password management, and configuration changes across all sites. Built-in cybersecurity features, including encrypted video streams and secure device authentication, help protect businesses against evolving cyber threats. **Command Enterprise Cloud** provides centralized video storage, secure remote access, and seamless scalability without the burden of on-site infrastructure.

AI-driven analytics add another layer of intelligence by integrating video with transaction data and IoT devices – helping enterprises find the video they need 90% faster.

AI-driven analytics add another layer of intelligence by integrating video with transaction data and IoT devices – helping enterprises find the video they need 90% faster. March Networks' Searchlight Cloud helps businesses detect fraud, theft, liability risks, and operational inefficiencies with real-time alerts and visual dashboards for enterprise-wide and site-specific intelligence – all tied to video.

By leveraging a comprehensive, flexible, and scalable enterprise VMS, businesses can protect assets, streamline operations, and make smarter decisions across all locations. That's why more than 1,500 financial institutions—including some of the world's largest, most complex banks—trust March Networks to manage their enterprise video.

Partner Insight

IDIS One Solution. One Company.

Unlocking High-Speed, High-Quality Video: How AI and Cloud Technology Revolutionize Surveillance

As organizations increasingly embrace cloud-based solutions, high-speed, high-quality video surveillance is more critical than ever. The cloud offers scalability, remote access, and centralized management, but maintaining superior video performance without compromising quality presents a unique challenge.

At IDIS, we combine advanced strategies and technology to deliver both high-speed streaming and exceptional video quality in the cloud. A key innovation behind our solutions is the **IDIS Intelligent Codec**, which reduces bandwidth and storage requirements without sacrificing video clarity.

Unlike traditional compression methods, the IDIS Intelligent Codec offers up to 50% greater efficiency, enabling businesses to stream high-definition video faster and store more footage in the cloud without costly infrastructure upgrades. This allows seamless access to live and recorded footage from anywhere, even under varying network conditions.

AI also plays a pivotal role in enhancing both video and audio processing. AI improves image quality by refining color, resolution, and clarity – even with minimal data. In video analytics, AI enhances detection accuracy by incorporating meta-processing frames. In audio, AI isolates human speech and amplifies background sound, enabling features like reverse noise canceling. These AI-powered improvements make security systems more responsive and precise.

At IDIS, we ensure our cloud-based solutions leverage AI and video compression technologies, helping organizations achieve efficient, scalable, high-quality video surveillance across industries.


Securitas
Technology

Securitas Group Insight

Securitas

Augmenting the Officer

How training and technology are transforming the role

Surveillance cameras, access readers, temperature monitoring tags, IoT devices – today's business environments are rich with connected security sensors that are continually processing security and operational data.

But there's another powerful sensor on-site: the security officer.

Across thousands of locations around the world, officers play a central role in day-to-day business operations – observing subtle changes in the environment, making decisions in real time, and actively preventing, responding to, and resolving security issues.

And despite advancements in technology and automation, the value of the security officer is only increasing, with their role becoming more – not less – essential to business security. That's why continued investment in officers and their evolving role within organizations is more critical than ever.

Here are three examples of what that looks like at Securitas today:

Turning guarding into intelligence-led protection

As more businesses adopt platforms for real-time risk intelligence, many still struggle to apply the "so what?" to their organization, including translating alerts into action. Officers, with the right training, can bridge that gap.

We've developed a pilot program to train officers in the fundamentals of intelligence, equipping them with the essential skills and knowledge of an intelligence operator. The program builds core competencies, such as developing an understanding of intelligence requirements to determine what matters to an organization, using different sources for collection – including engaging with local emergency services – and how to use intelligence analysis to stay ahead in today's evolving threat landscape.

Most importantly, officers learn how to embed intelligence into day-to-day decision-making on-site, helping organizations respond faster and avoid bottlenecks at the local level.

Learn more at securitas.com

Developing specialized expertise in data center security

Another specialized training program is preparing more than 10,000 officers to meet the complex demands of one of the world's most critical and fastest-growing industries: data centers.

Launched in 2024 and accredited by the Holistic Information Security Practitioner Institute (HISPI), the program trains officers to become Certified Data Center Security Professionals. It's designed to address the specific risks and requirements of this sector – recognizing that the traditional one-size-fits-all approach to guarding is no longer enough for high-stakes, high-security environments like data centers.

This type of advanced knowledge and specialization makes officers increasingly vital resources that further enhance a data center's security posture and bolster its resilience.

Optimizing officer routes and staffing

While advanced training prepares officers for more strategic roles, technology plays an equally important part in streamlining their impact and driving significant efficiencies for organizations.

In several European countries, we've introduced AI models that enhance how we deploy officers by factoring in commute times, skill alignment, and long-range staffing forecasts. In the Berlin metropolitan area alone, optimized routing has the potential to reduce daily commuting distances by 44%.

AI is also helping us optimize guarding office locations, which has already led to a 10% average reduction in driving time in Germany, generating indirect cost savings for the organizations we serve.

All of this amplifies the impact of officers, leading to greater efficiency, faster support, and ultimately, more satisfied clients.

Reimagining the role of the officer

Each of these examples points to a broader shift in how we think about security – and about people.

The most effective security strategies aren't built on technology alone. They're powered by people – trained, trusted, and connected – who can plug into an organization's security ecosystem and keep it running smoothly.

And as the industry continues to evolve, our commitment to those people remains at the heart of everything we do. With advanced training, specialized expertise, and AI, we're empowering officers with the tools to face the future, while strengthening the resilience of the organizations they help protect.

Action Plan for Security Professionals

"The future of security is shifting toward real-time, proactive management, driven by AI, data integration, and other network technologies. By augmenting human agents with AI, organizations can enhance incident response, improve efficiency, and anticipate threats with greater accuracy. As organizations adopt these powerful technologies, it's critical to also ensure network security, privacy protection, and adherence to regulations and standards for the responsible use of AI."

Mike Beattie | CIO & SVP Information Global Technology
Securitas Technology

1 Review Incident Response Protocols

Conduct a comprehensive assessment of how events are monitored and managed across the organization, from alarm response processes to routine security tasks. Understand the capabilities roadmap of the organization's security service provider and examine opportunities to create an information ecosystem for automations, agent support, and analysis.

2 Prioritise Investment in Proactive Technologies

Allocate resources in the security budget for implementing cutting-edge technologies and data integrations that enable proactive threat detection, incident response, and analysis. Consider AI-driven automation and remote services to transform security operations into a forward-thinking, responsive system.

3 Embed AI Into Incident Response Protocols

Collaborate with internal stakeholders to create a strategic plan for integrating AI into incident response protocols. Focus on augmenting existing processes with AI solutions, while ensuring compliance with regulatory, legal, and ethical standards.

5

Security Systems Driving Value & Organizational Impact

The bedrock importance of security has always been well understood. It's a fundamental human need that helps to ensure the safety and well-being of individuals and organizations alike.

Security systems have consistently delivered value because they help organizations protect their people and assets and help prevent life-altering disasters. Security and loss prevention professionals are engaged in an activity that is essential to human thriving, providing peace of mind and stability in an ever-changing world.

Now, there is potential to do even more. Security systems generate a wealth of information that organizations can use to deliver different kinds of value, opening new possibilities for enhancing operational efficiency, improving decision-making, and driving innovation. It's a fresh perspective on the return on investment businesses can achieve through security technology, transforming it from a protective measure to a strategic asset that contributes to overall success.

Security Data Contributing to Business Optimization

We live in a data-driven world. Organizations are seeing a need for analytics across their activities, and security is no exception. We are working with clients to integrate data from multiple security systems to better analyze patterns in security activity and uncover insight that support broader business improvement efforts.

Improving customer and employee experience is a

Top 5

Driver of security technology[1]

Data Integration Driving Insights

There is a growing appetite among organizations to combine data from disparate security systems to gain a greater, more holistic understanding of how their security systems are interacting. This intent is focused on identifying trends in the data that can help to make sense of when and why security incidents occur.

For example, security managers could leverage integrated data from access control logs and video surveillance systems to uncover critical insights into staff safety. By analyzing this data – made even easier with the help of AI – it becomes possible to pinpoint specific locations and times where staff members are most susceptible to incidents of violence.

Organizations are also beginning to integrate their security data with data from internal platforms (operational, financial, etc.) and external sources such as cyber threat and risk intelligence to create a more holistic view of organizational risks and performance. The≈analysis via AI of event correlation among these diverse data sources opens the possibility for new kinds of alerts on security threats but also other business activities.

[1]Third-party blind survey of 575 security professionals with decision-making authority for security technology in Australia, France, Germany, Sweden, the United Kingdom, and the United States. Conducted February & March 2025.

The Shifting Regulatory Landscape for AI and Cybersecurity

Two regulatory trends require the attention of security professionals and their peers in IT, Legal, and Compliance. The EU AI Act, enacted in August 2024, provides a framework for responsible AI use, with compliance starting in February 2025 for some applications. Organizations must determine how their use of AI is classified under the Act and adhere to its requirements. In the US, the Colorado AI Act is the first general AI legislation, while states like New York, Florida, and Utah have more focused laws. Globally, Australia, Canada, and the UK among others are also developing legislation.

Cybersecurity regulations are also evolving, with the EU's Network and Information Security 2 Directive (NIS2) effective from October 2024. This directive mandates enhanced cybersecurity standards for critical sectors, including physical security systems. In the US, cybersecurity laws vary, with federal regulations targeting sectors like banking and critical infrastructure, and state privacy acts affecting security measures, such as video footage protection.

Enhancing Client Experiences

By understanding client interactions and preferences through their security data, businesses can tailor their services and environments to help enhance client experiences.

This is especially important in retail settings where insights on client behavior can help identify busier areas of a store and optimize product placement, an action that can directly contribute to influencing increased sales.

In the world of hospitality, a hotel can program access control systems with pre-collected guest preferences, such as room temperature and lighting settings, and automatically adjust these upon check-in to create a personalized and comfortable stay.

Making these types of adjustments based on data-driven insights is an effective way to drive success while fostering continued client satisfaction and loyalty.

Optimizing the Workplace

Business security systems continuously capture valuable data, offering insights into building usage with every interaction, such as access-controlled doors opening, or alarm systems being disarmed. In corporate offices, access control and surveillance data can reveal patterns in employee movement and space utilization, enabling organizations to optimize meeting room bookings, adjust lighting and heating schedules, and redesign office layouts for enhanced efficiency and improved employee satisfaction.

The challenge lies in analyzing this data, a task that demands time and focus, which security and facilities managers often lack due to other priorities. Technologies like AI can assist by efficiently processing large data sets and delivering actionable insights quickly, simplifying the process.

Additionally, integrating environmental sensors into business security systems allows organizations to monitor additional aspects of the workplace. For instance, in schools, smart sensors can detect air quality changes and alert security teams to unauthorized vaping or the presence of chemicals like THC, the active ingredient in cannabis.

Partner Insight

Responsible AI in the Modern Security Industry

As AI continues to shape the security industry, it's essential for businesses to understand its risks and advantages. Security providers have a head start in addressing AI-related challenges due to their long history with AI solutions.

However, the responsibility of using AI extends beyond legality—it requires transparency and ethical considerations. The Organization for Economic Cooperation and Development's framework for human-centric AI highlights the importance of ensuring customers understand how AI works and its limitations, fostering trust with partners and clients.

AI in security primarily aims to automate tasks and provide actionable insights. While AI-driven automation improves efficiency, it's crucial to assess potential risks, such as the consequences of an AI error. Transparency about AI capabilities allows businesses to make informed decisions and manage risks effectively, especially in critical sectors like manufacturing and critical infrastructure.

Responsible AI deployment requires both ethical design and mindful use.

Additionally, AI systems must be evaluated for biases and limitations, particularly when analyzing data under varying conditions. As new AI technologies, like generative AI, emerge, robust testing in real-world scenarios is necessary to understand their impact fully.

Ultimately, responsible AI deployment requires both ethical design and mindful use. Security providers must ensure AI isn't misused and build strong, transparent relationships with partners. By doing so, they can gain trust and remain competitive as AI evolves.

Partner Insight

3xLOGIC

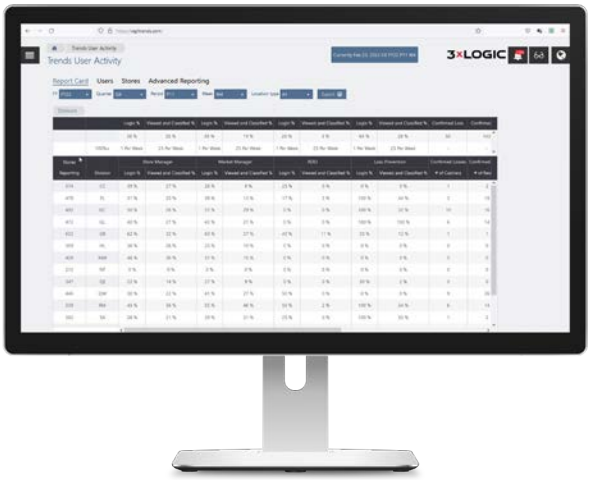
Leveraging Security Data for Business Intelligence

The data from video surveillance, access control, sensors, and other security systems hold a great deal of business value, not only to improve security but to understand business performance.

In retail, hospitality, and related sectors, for example, fraud and shrinkage are long-standing problems – in convenience store and restaurants, employee fraud fuels a staggering 25-45% of losses. But what are the specific drivers of those losses and what specific steps can organizations take to reduce them?

A new generation of business intelligence tools designed for security data now support sophisticated analysis of trends and better situational awareness. Solutions such as **3xLOGIC's VIGIL TRENDS** use both rules-based analysis and inference to help identify patterns of internal theft, optimize employee performance, and improve overall process efficiency.

One client saw a drop in average fraud per identified employee from $800 to $500.



Data need not be limited to security systems. Integrating sales information, weather and other sources enables even richer analysis, including store comparisons, sales conversions, dwell time data and traffic counting.

This insight can drive direct financial benefits. One 3xLOGIC client saw a drop in average fraud per identified employee from $800 to $500 over three years. For a chain with a thousand locations, that could mean tens of thousands in loss prevention per year.

Ultimately, effective security-driven business intelligence enables organizations to stay ahead of risk, protect their bottom line, and build a culture of integrity.

Partner Insight

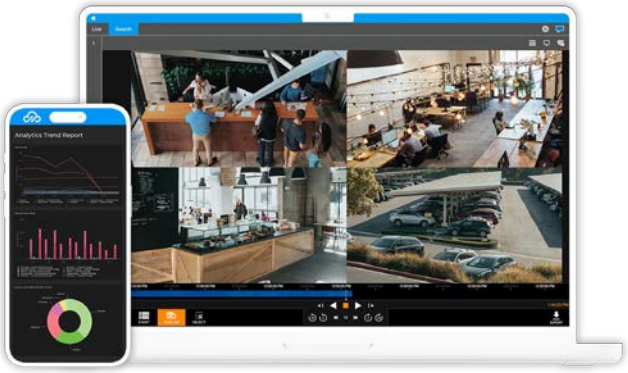
OpenEye

Unlocking Business Insights with an Open Video Platform

Choosing an open platform for cloud video allows you to harness disparate data points across your operations and marry them to video for a more complete view of your business. These unified solutions help drive more informed decision-making, create operational efficiencies and improve your bottom line.

An open platform enables seamless integration of business systems, such as access control, environmental sensors, point of sale, business intelligence, and more, to improve business security and operations.

These integrations deliver actionable intelligence beyond the historical use cases for video. In commercial production, managers can monitor inventory levels and employee activity, ensuring efficiency. Service operations benefit from insights into customer behavior patterns alongside transaction data, enabling strategic adjustments to improve performance and revenue. Marketing and sales gain a deeper understanding of customer interactions and preferences, allowing them to tailor efforts for maximum impact.



By connecting and analyzing data from the systems that matter most to your business, an open platform delivers a more complete end-to-end security solution. Connected security adds value across an entire organization by providing the details needed to surface valuable insights and in turn, make better decisions. By achieving a more complete view of your business, you deliver a unified solution that fortifies security, improves your bottom line, and propels your business forward.

> Connected security adds value across an entire organization.


Securitas
Technology

Promoting Sustainability & Streamlined Operations

Sustainability has become a central commitment and operating parameter for many organizations. Companies are setting specific sustainability goals, aiming to measure and reduce their environmental footprint. The security technology industry is responding to this shift with an increasing focus on efficiency, scalability, and flexibility – meaning organizations can realize concrete benefits while delivering on their sustainability commitments.

Realizing the Benefits of Remote Services

One significant trend in the industry is the remote-first approach to service and maintenance. By prioritizing solutions and services with strong remote capabilities, companies can reduce the need for physical travel and system inspections, helping to cut down on unnecessary carbon emissions.

Improved remote capabilities is one of key advantages offered by cloud-based security systems, which are progressively becoming the preferred choice for many organizations. The ability to manage security operations remotely – especially for businesses with multiple locations and numerous systems – allows security managers to oversee all security activities from a single digital interface. This provides increased clarity and control over operations, as well as helping to cut costs associated with physical attendance.

In addition, remote monitoring and maintenance allow for quicker response times and less downtime, boosting operational efficiency and supporting sustainability efforts. This approach is a win-win for clients and service providers: improved service delivery, more efficient operations, and a smaller environmental footprint.

> “Many organizations now prioritize sustainability as a core business objective. By collaborating with our clients and partners, we’re focused on leveraging security technology to help them reach these goals.”
>
> **Kristi Keating | Global VP, Sustainability**
> **Securitas Technology**

Actively Seeking Greener Solutions

Innovations in security technology are also playing a crucial role in promoting sustainability. For instance, the development of power-efficient cameras and the use of LEDs in equipment is a direct response to the need for greener solutions. These technologies consume less energy, reducing the overall power demand and helping organizations lower their carbon footprint. By integrating such sustainable technologies, companies can achieve their security objectives while also supporting their environmental goals.

Efficient Tracking of Sustainability Data

Organizations participating in frameworks like the Science Based Targets initiative (SBTi) are required to understand and document their environmental impact comprehensively. This includes the power consumed by security systems, which is typically included in the indirect emissions an organization generates through its use of electricity. Calculating these emissions requires knowing the power consumption of each device and how the electricity used to run them is generated.



The security industry is beginning to facilitate this kind of analysis. Working with its strategic partners, Securitas Technology is leading the effort to include power consumption information for all equipment in client quotes (beginning in North America) along with an estimate of emissions in CO2 equivalent based on the typical mix of electricity generation in each country or region.

The same techniques can be used to document emissions from existing equipment, with access to the data through a technology lifecycle management tool that stores the full installation, service, and maintenance history of each device.

As companies continue to set and pursue their sustainability goals, the security industry can support these efforts, ensuring that both security and sustainability go hand in hand.

Sustainability as a Security Priority[1]

33% Of security professionals participate in sustainability activities

48% Say sustainability is important or very important in technology selection

The drive for sustainability is reshaping the security industry, leading to innovations that offer both operational and environmental benefits. By adopting remote-first strategies and integrating power-efficient technologies, organizations can streamline their operations while contributing to a more sustainable future.

[1]Third-party blind survey of 575 security professionals with decision-making authority for security technology in Australia, France, Germany, Sweden, the United Kingdom, and the United States. Conducted February & March 2025.

Partner Insight

Supporting Efficient Workflows with Simple, Secure Systems Access

In modern high pace work environments, people require fast, frictionless access to the physical and digital systems around them without compromising security.

Some industries, such as healthcare, feel this acutely. Healthcare providers need swift but also secure access to patient information and systems, while administrators require tools to manage credentials and streamline processes effectively.

Traditional access control methods like passwords and PINs are vulnerable to theft, loss and misuse. They also fall short in providing the level of assurance needed in healthcare environments where mistakes or fraud can have life-altering consequences.

A newer generation of access control technology empowers healthcare and other organizations to effectively balance ease of access with security and control. A unified platform for identity authentication, such as HID OMNIKEY, enables quick and secure log-in to workstations, saving time and improving data protection.

Such systems support various card technologies and integrates seamlessly with existing IT infrastructure, ensuring seamless access to patient information while complying with healthcare data protection regulations.

Advanced biometric authentication through a platform like **HID DigitalPersona® for Healthcare** is another solution that effectively addresses the unique access challenges of healthcare. Single sign-on using biometric factors such as fingerprints or facial recognition streamlines access to multiple healthcare applications, systems, and physical spaces. This enhances security by eliminating shared or weak passwords, improves user experience and productivity for healthcare staff, and supports data security and privacy compliance requirements. Additionally, it delivers significant cost savings by reducing password management overhead.

By streamlining workflows and enhancing security, effective access control allows healthcare providers to spend less time logging into systems and more time providing care and improving the patient experience.

Partner Insight

ASSA ABLOY
Opening Solutions

How Security Technology Fits into Sustainable Buildings

Engineers and architects evaluate a building's sustainability footprint by examining the entire structure to identify areas of energy use or loss. Traditionally, these assessments have focused on HVAC systems and insulation. However, as new products emerge, attention is shifting to other high-energy areas, including door-dense environments and the energy consumption of locks and access control devices.

Most buildings already have network infrastructure in place. By leveraging these existing IT networks for security applications, such as access control, we can optimize energy usage, reduce cabling and labor costs, and maximize the value of original infrastructure investments. IP-enabled Power over Ethernet (PoE) and Wi-Fi locks facilitate this process. Utilizing the existing IT infrastructure allows facilities to expand access control systems easily and cost-effectively. Integrating security technology into sustainable building practices enhances both efficiency and sustainability.

Building owners are establishing sustainability goals to reduce their carbon footprint. They actively seek products that align with these goals and want to partner with manufacturers with similar environmental objectives. Customers increasingly demand transparency about where products are made, the materials used, and the energy used throughout the product's life cycle.

We provide this level of transparency to our customers by utilizing our **Sustainability Compass** for every new product developed, aiming for a lower environmental impact than previous products. We issue third-party-verified sustainability documentation to help educate our consumers and assist them in achieving green certifications to meet their goals. We enable customers to incorporate sustainability into every building project, bringing more responsible products to the market.

Partner Insight

Exploring the ROI of Security

Today's security systems are moving beyond traditional access control and surveillance, enhancing business operations and positively impacting Return on Investment (ROI). It's crucial for users and security integrators to measure and communicate these benefits to stakeholders, transforming security from a reactive cost center to a proactive strategic partner, and increasing buy-in for future investments.

How video surveillance and access control can deliver ROI

With AI and analytics - often operating in the cloud - repetitive and time-consuming tasks can be automated. Alerts can be generated on unusual behavior, leaving operators free to work on other tasks. This improves team efficiency and situational awareness.

Response management is also boosted, as ground teams can be directed based on attributable data such as the color of vehicles or clothing captured on camera, or repeated attempts to access protected areas by unauthorized persons. Cameras can track objects as they move, and hand over the monitoring of situations and objects between different devices. This helps intrusion response and perimeter control.

Longer term, insights on site usage generated by access control systems can influence how a building is used more efficiently, influencing signage and route planning and even helping to refine maintenance and cleaning schedules for high-traffic areas.

Getting started

Partnering with stakeholders in other departments allows security leaders to identify areas where access control and video deliver added value. It also supports the generations of wider metrics that security teams may otherwise be unaware of, such as shorter checkout or wait times, scheduling optimization, gaining savings, making health and safety improvements and managing energy usage.

Consolidating security solutions into a single management platform therefore makes it easier to unlock value-added insights. As everything is in one place, data from video, access control, detection and perimeter control systems can be used to identify improvements and efficiencies. It also makes it simpler to keep all stakeholders updated, so the ROI is clear and understood.

Securitas Group Insight

> “When staff feel protected, they are more likely to stay in their roles, reducing turnover and ensuring better care.”

Bill McCarthy, President of Securitas Healthcare

Securitas Healthcare

Building a Culture of Employee Safety

Lessons from the frontlines of healthcare

Violence in healthcare settings is a well-documented and global problem, identified by bodies ranging from the World Health Organization[1] to the European Union[2] and the US Centers for Disease Control and Prevention[3]. In the US, healthcare is the most hazardous working environment for non-fatal violence, accounting for an astonishing 73%[4] of all instances.

Because of this, the healthcare sector has developed a robust approach to mitigate the risk of workplace violence from which other sectors can learn.

“Protecting healthcare workers requires a multi-faceted approach that evolves alongside emerging threats. By integrating advanced security technology with staff training, we can create safer environments for both caregivers and patients,” observes Ara Kouchakdjian, VP, Data Intelligence & Healthcare Innovation at Securitas Healthcare.

Learn more at securitashealthcare.com

[1]“Violence and harassment.” World Health Organization, 2025. https://www.who.int/tools/occupational-hazards-in-health-sector/violence-harassment
[2]“Violence in the workplace.” Eurofound, 27 February 2023. https://www.eurofound.europa.eu/en/blog/2023/ violence-workplace-women-and-frontline-workers-face-higher-risks
[3]“Prioritizing our Healthcare Workers.” Centers for Disease Control, May 29, 2024. https://blogs.cdc.gov/niosh-science-blog/2024/05/29/hcw_violence_mh/
[4] “Workplace Violence in Healthcare.” 2018. Bureau of Labor Statistics, April 2020. https://www.bls.gov/iif/factsheets/workplace-violence-healthcare-2018.htm

A Multi-Layered Approach to Security

Ensuring a secure healthcare environment requires perimeter security, controlled access, real-time monitoring, and rapid response coordination. Securitas Healthcare is seeing more facilities developing workplace violence steering committees involving legal, risk management, security and clinicians to develop a holistic, multi-layered, security strategy.

1

Strengthening Perimeter Security & Smart Access Control

Hospital security begins at its perimeter. Video surveillance and video analytics monitor high-risk areas like parking lots and entry points. Motion detection and facial recognition provide real-time threat detection, allowing security teams to intervene before incidents escalate.

Weapons detection systems at any entrance can prevent dangerous situations before they enter the facility. Badge-based authentication ensure only authorized personnel access sensitive areas.

To enhance visitor management, hospitals also implement real-time tracking and notification systems giving staff visibility into who is entering and leaving the facility.

2

Protecting Staff: The Key to Safety and Retention

Even with strong perimeter defenses, healthcare workers remain vulnerable. Violence is unpredictable; security can't always be everywhere.

For this reason, hospitals frequently invest in staff protection solutions such as wearable badges with built-in panic buttons, like those offered by Securitas Healthcare's Staff Protection solution. These allow employees to discreetly call for help during staff duress incidents.

3

Investing in De-Escalation Training and Emergency Preparedness

Technology alone isn't enough – staff need skills to manage aggressive situations. De-escalation training helps employees recognize early warning signs and defuse tense interactions.

Hospitals also routinely conduct emergency preparedness drills. Training for active assailant scenarios, mass casualty incidents, and workplace violence ensures staff understand their role in a crisis.

"When staff feel protected, they are more likely to stay in their roles, reducing turnover and ensuring better patient care," says Bill McCarthy, President of Securitas Healthcare. "By investing in proactive security measures and developing a holistic security strategy, hospitals create an environment where staff feel valued, protected, and empowered to provide the best possible care."

Action Plan for Security Professionals

> Security technology is now a driver of business value, in addition to delivering on its core mission of safeguarding people and property. Strategic investments in AI-driven solutions and analytics, remote services, and sustainable technology can help organizations enhance operational efficiency and reach their security, business, and environmental goals.

Doug Walsh | Global VP, Technology Strategy
Securitas Technology

1 Develop ROI-driven Use Cases for Security Data

Working with operational, finance, and other functional areas, review how data from security systems can support specific organizational goals (for example, reducing shrinkage, reducing wait times, identifying safety risks, etc.). Define these uses cases and create the data and analysis infrastructure – likely leveraging AI – to unlock insights, enhance business efficiency, and demonstrate the extended value of security investments.

2 Leverage Remote Services via the Cloud

Find out about the growing range of remote services available to support security systems – from remote management to preventative maintenance – and factor this into the cloud migration roadmap. Consider how a remote-first approach can contribute to enhanced efficiency and sustainability.

3 Understand How Security Can Support Sustainability Goals

Engage with internal sustainability leaders to define what information is required from the security function. This may involve documenting the power consumption of security devices, which constitutes a major part of the environmental footprint of security technology. Work with security technology integrators and vendors to establish a process for efficient reporting of this data so that security operations stay aligned with sustainability objectives.

About Securitas Technology

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

With more than 13,000 colleagues in 40 countries, our mission is to make the world a safer place through cutting-edge security technology and an unwavering commitment to client success.

Securitas Technology

See a different world

3800 Tabs Drive
Uniontown, OH 44685

securitastechnology.com