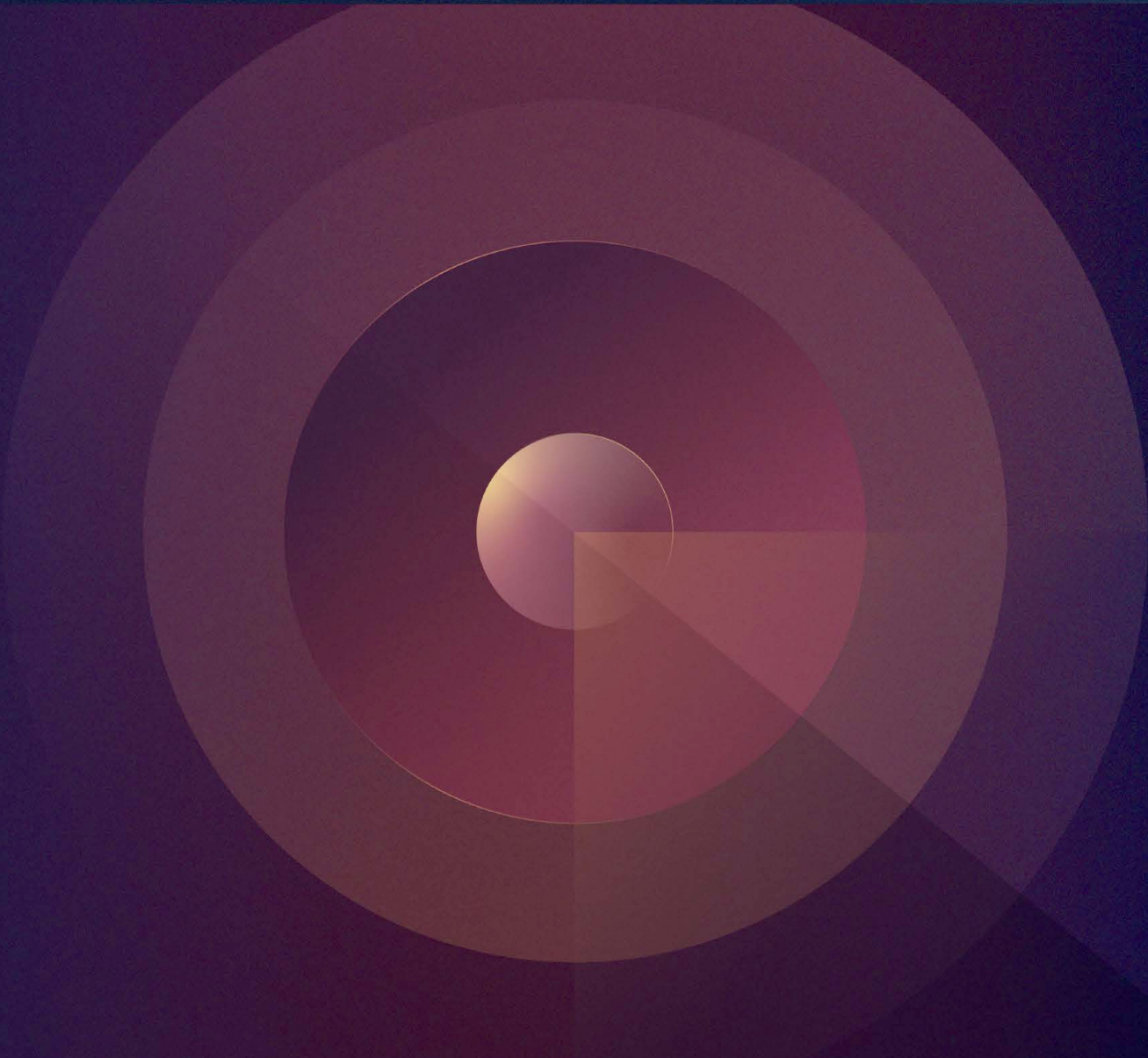




State of Physical Security 2026

Collaborative transformation

Genetec[™]



Foreword

Rapid technological innovation is reshaping the future of physical security.

Organizations are now discovering how new technologies enhance the safety and responsiveness of their security systems. As capabilities expand, so do the possibilities. The real impact of these technologies, however, will depend on how they are applied.

This report explores how the industry is adapting and how strategic innovation¹ is redefining what's possible in physical security.

Technology must be managed and deployed with intention, not for its own sake. AI-driven analytics, for example, add value only when paired with responsible data practices and clear operational goals. Similarly, cloud adoption succeeds when it strengthens resilience and enables collaboration, not when it adds complexity. Success depends on aligning technology with purpose, ensuring it serves people, processes, and outcomes rather than existing as an end in itself.

As the industry continues to transform, collaboration is critical among physical security teams, information technology (IT) teams, and solution providers, including channel partners and manufacturers. Together, they can bridge gaps, align systems, and build smarter, more resilient approaches to protection. This partnership is key to unlocking the full potential of modern physical security operations.

We're pleased to share the findings of this sixth edition and hope you find the insights both engaging and valuable.

The Genetec Team

1. Strategic innovation, in this report, refers to the intentional application of new ideas and technologies to address today's challenges and shape the future of physical security. It aligns innovation with long-term objectives, driving meaningful progress while enhancing operational effectiveness.

Contents

Foreword	2
Table of contents	3
About the research	4
Executive summary	7
Physical security as a strategic function	8
The value in doing more	9
A collaborative business partner	14
IT's growing presence in physical security	15
The transformative effects of IT's role	16
The digital revolution of security operations	17
Where unification meets cyber risk	18
The cloud as an enabling force	22
Physical security data: A shared asset	29
AI and analytics: From sensing to sense-making	31
The 2026 forecast	37
Changing market dynamics	37
The economic landscape's impact on staffing	40
Adapting project priorities for 2026	43
From vendors to value partners	45
Key takeaways	46
Appendix	49
Appendix 1 – Survey methodology	49
Appendix 2 – Respondent information	50
Appendix 3 – Respondent demographics	51
Appendix 4 – Respondent comments	53

About the research

For the sixth annual State of Physical Security report, Genetec Inc. surveyed physical security professionals worldwide from August 18 to September 15, 2025. After data validation and cleansing, 7,368 fully completed surveys were analyzed. The findings capture the state of the industry in 2025 and signal priorities for the year ahead.

In this report, you will gain insights on:



Where organizations invested in 2025



Which technologies gained traction



How priorities are evolving as the industry matures

Our survey at a glance*

Fieldwork

August 18 – September 15, 2025

Respondents

7,368 across six regions

Audiences

- End users
- Channel partners
- Consultants
- Manufacturers

Languages

English, French, German, Spanish, Portuguese, Japanese, Korean, Italian

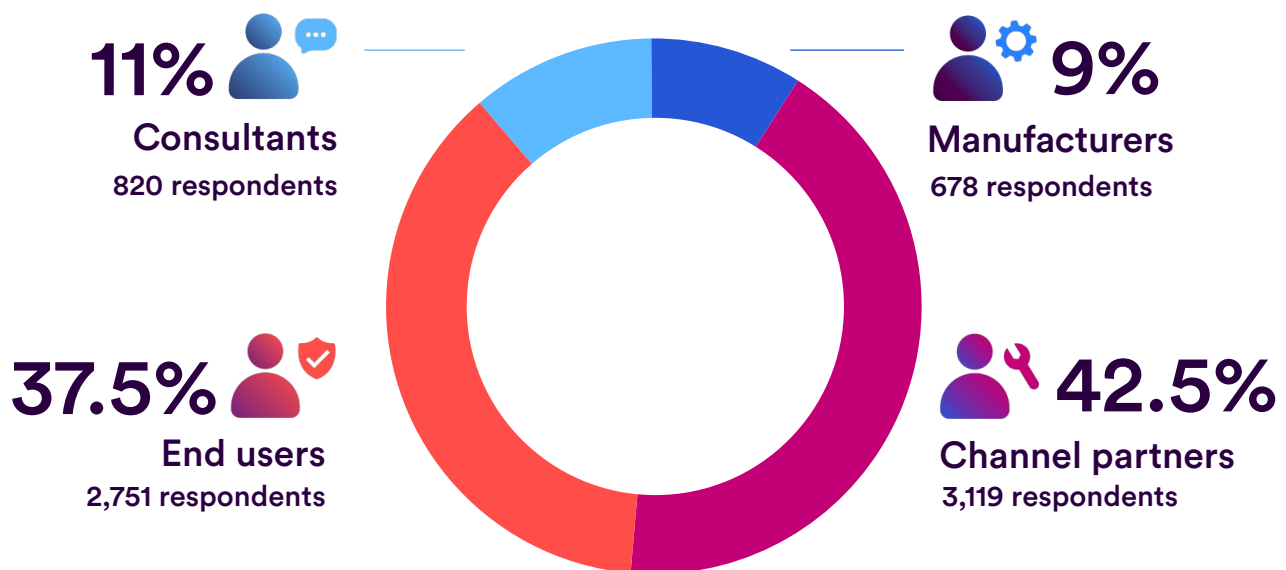
Method notes

- Fully completed surveys only
- Percentages rounded
- Multi-select questions may exceed 100%

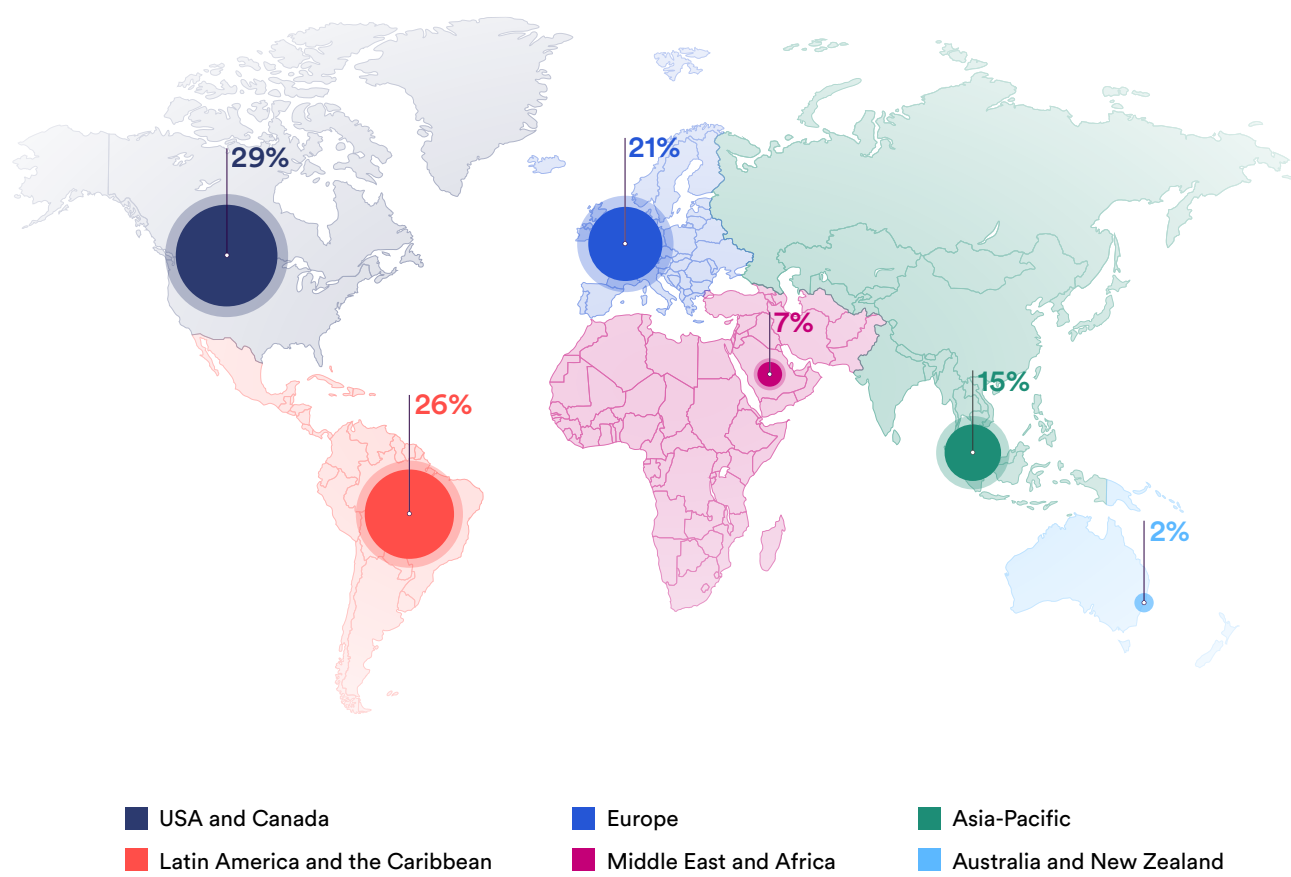
*For further details about the survey methodology and respondent demographics, please see the appendices.

About the survey participants

- The 7,368 participating security professionals include end users, channel partners, manufacturers, and consultants.
- Each group gives a glimpse into their market perspectives and how their operations and use of technology are changing.
- The groups completed surveys tailored to their specific roles, letting them share their distinct insights, priorities, and views on physical security.
- The term “channel partners” refers collectively to integrators and installers.
- These groups are mentioned throughout the report. If a chart or table doesn’t specify the group (end users, channel partners, manufacturers, or consultants), it represents responses from all participants.
- Survey responses were gathered through in-person events, digital promotions, and opt-in email lists from third parties.
- Only fully completed surveys submitted by individuals within the targeted population were included in the final analysis.



Geographical distribution of respondents



PROPORTION OF RESPONDENTS BY REGION.

Executive summary

The Genetec State of Physical Security 2026 report presents survey data on how technology is redefining physical security. Findings show it is increasingly viewed not just as protection for people and assets, but as an enterprise function supporting resilience and business value. Respondents highlight an industry embracing innovation, aligning more closely with IT, and investing in modernization.

These insights reveal distinct opportunities and challenges:

Unified and integrated systems dominate, enabling holistic security management and better decision-making

Interest in AI adoption has doubled among end users, driving demand for advanced analytics and automation tools that improve operational efficiency

Cloud adoption in the form of hybrid models is gaining momentum, as organizations look for flexible, scalable solutions

Workforce challenges persist, though training programs and automation are being introduced to bridge capability gaps

Collaboration between IT, security, and solution providers—including channel partners and manufacturers—is central to navigating new risks, enhancing decision-making, and turning security data into actionable insight

Looking ahead, findings indicate that organizations are prioritizing investments that modernize their physical security systems and offer long-term value. End users increasingly seek strategic partners who can provide not just technology, but expertise, trust, and stability in a dynamic industry.

Physical security as a strategic function

“With the rapid development of science and technology, new security threats emerge one after another. This requires physical security enterprises to have strong technological capabilities and a continuous sense of innovation, to cope with new challenges.”

– Channel partner respondent



The industry has entered a new era of disruption and opportunity. This year’s survey results indicate a fundamental shift in how physical security departments operate, invest, and deliver value. Operations are now being reshaped as technology

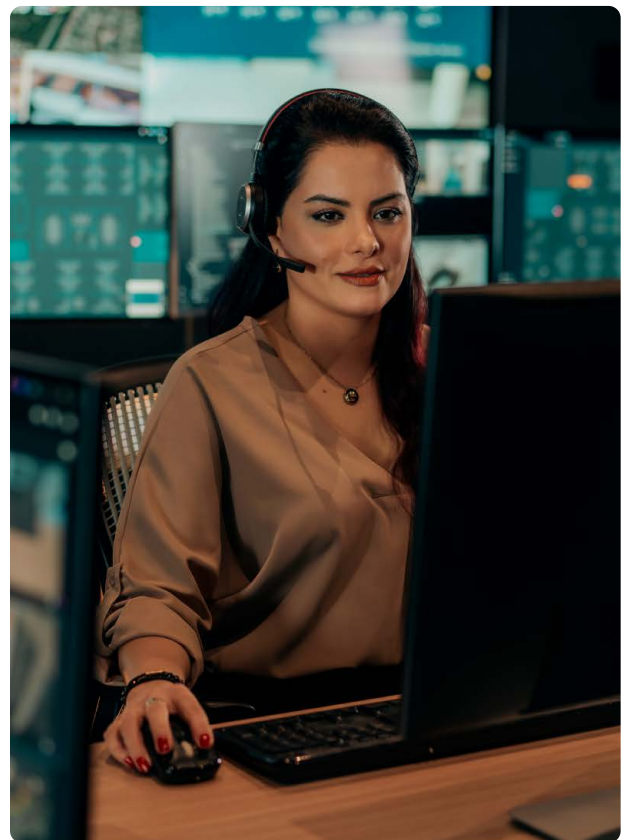
drives new ways of working and stronger decision-making. As a result, physical security is becoming a more enterprise-focused function that is critical to ensuring safety while contributing to organizational success.

The value in doing more

“Customers are increasingly expecting security systems not only to protect but also to deliver operational insights and business value.”

– Channel partner respondent

Physical security technology is no longer about individual tools. Survey findings point to a shift in how physical security systems are deployed and valued. Previously independent components (such as video management and access control systems) are combined to help with operator efficiency. The survey indicates this evolution goes beyond core systems to include data visualization and tools that enhance operations. Value is now being assessed by how these systems help users and organizations achieve more. Advanced capabilities such as video analytics, intrusion, and perimeter protection are expected to be built in, rather than added on.



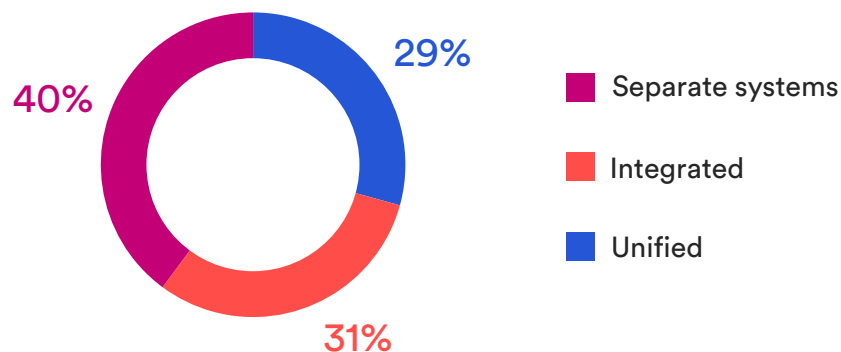
“Security is becoming a strategic function. When systems deliver intelligence alongside protection, they empower enterprises to innovate, adapt, and lead in an era of constant change.”

Christian Morin

Vice-President, Product Engineering
Genetec Inc.



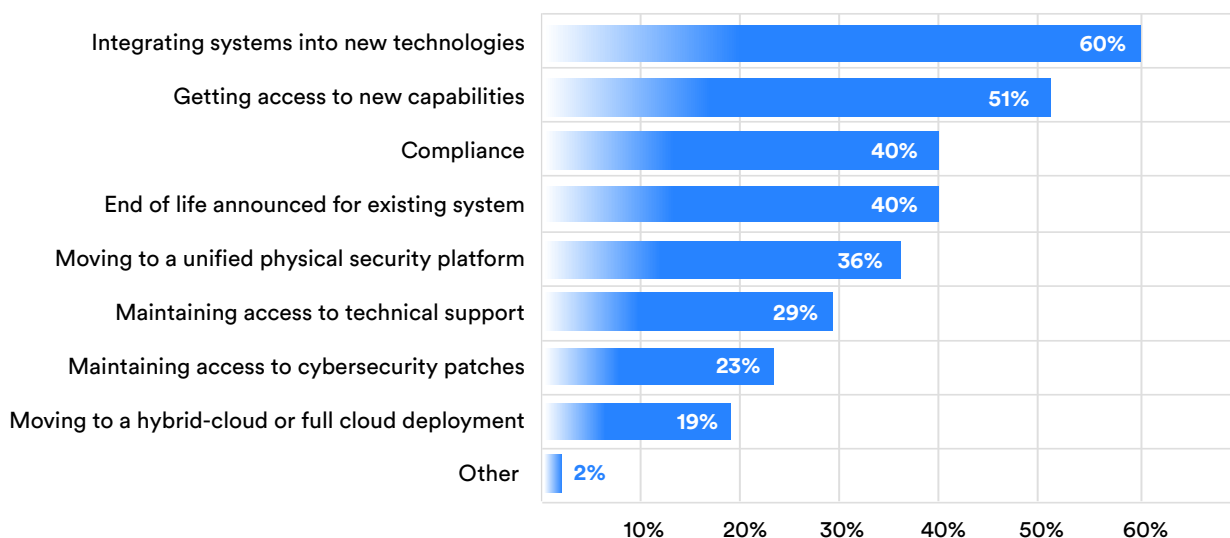
Which describes your video surveillance and access control implementation?



More than 60% of respondents are running unified or integrated systems.

Survey results indicate that the top reason for replacing legacy technology (cited by 60% of respondents) is to integrate systems with new technology. Users are seeking interconnected, modern solutions that can deliver greater value.

In your experience, what is the primary motivation of customers replacing legacy systems?



MULTIPLE RESPONSES ALLOWED; PERCENTAGES REFLECT SHARE OF RESPONDENTS SELECTING EACH OPTION.

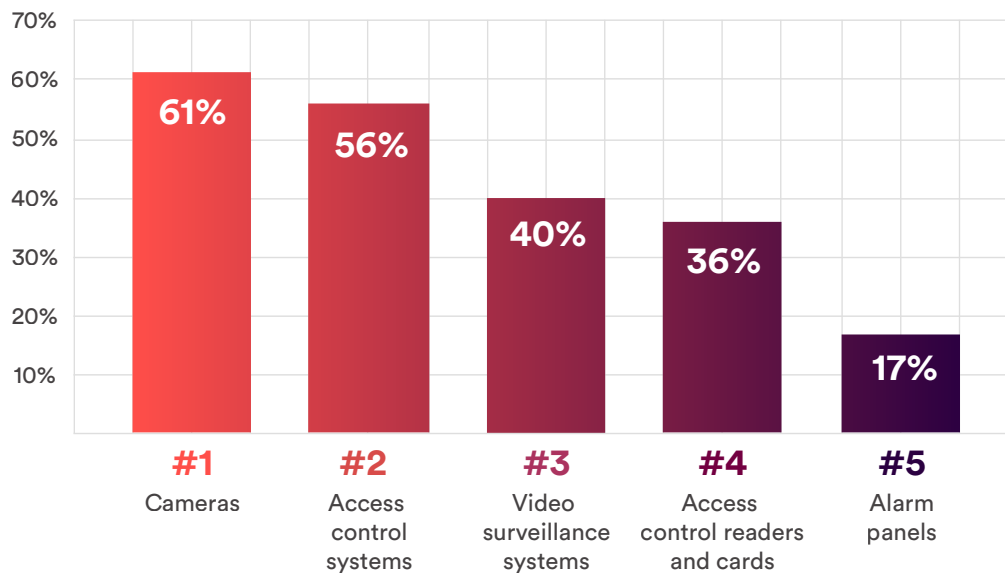
Channel partners and manufacturers also report that their customers are prioritizing upgrades to get access to new capabilities and gain more value from existing investments. There is growing demand to update

or replace core systems, which allows users to take advantage of new integrations, features, and connected capabilities such as AI-powered investigations or remote monitoring.

Insight

91% of channel partners and manufacturers said the demand to add new technologies to existing systems increased or stayed constant in 2025.

Top 5 systems replaced 2025



MULTIPLE RESPONSES ALLOWED; PERCENTAGES REFLECT SHARE OF RESPONDENTS SELECTING EACH OPTION.

Top motivations for replacing a system

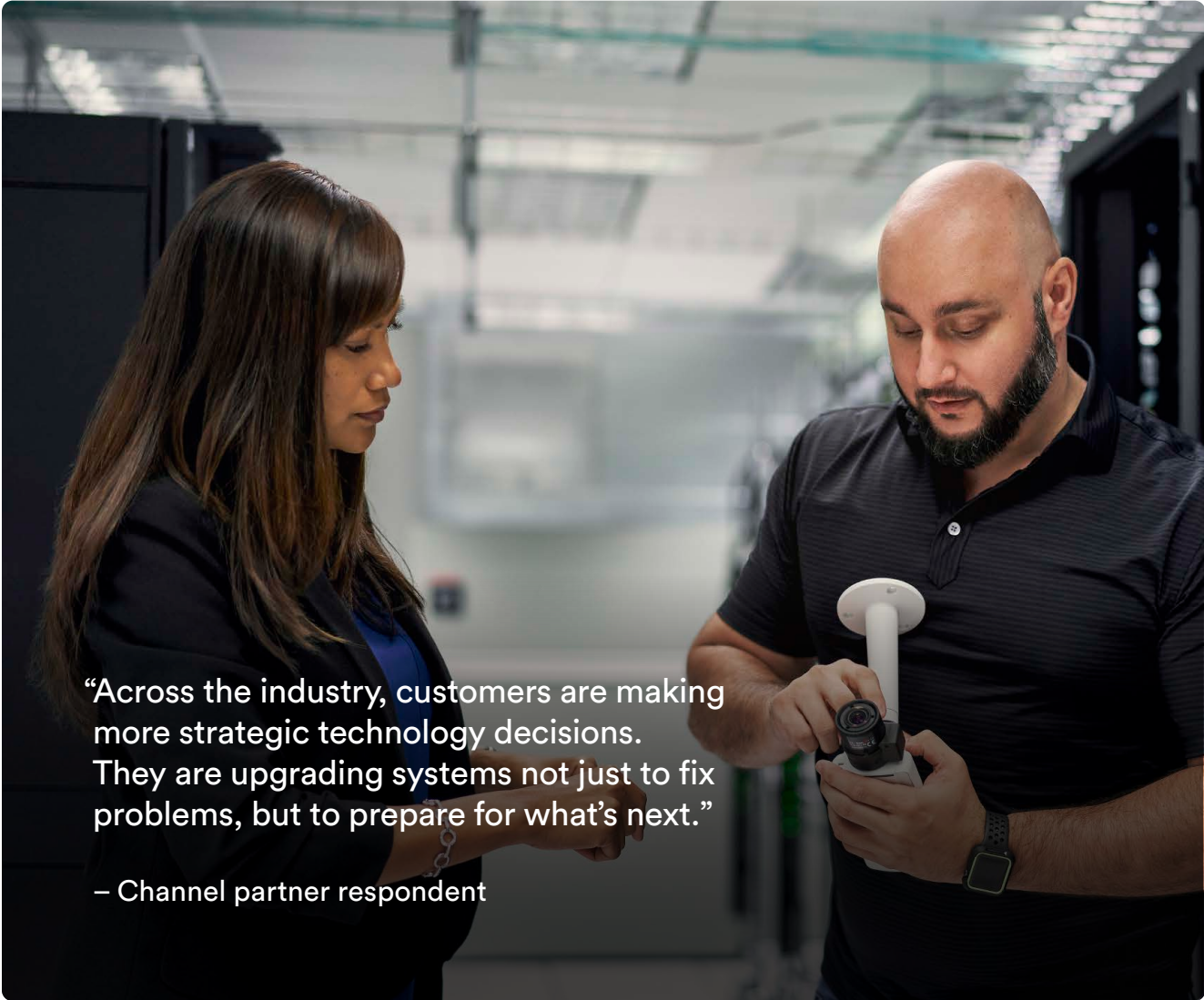
60%

of respondents said integrating systems into new technologies

51%

of respondents said gaining access to new capabilities

MULTIPLE RESPONSES ALLOWED; PERCENTAGES REFLECT SHARE OF RESPONDENTS SELECTING EACH OPTION.

A woman with long dark hair and a man with a beard are in a server room. The man is holding a small white device with a camera lens and they are both looking at it. The background shows rows of server racks.

“Across the industry, customers are making more strategic technology decisions. They are upgrading systems not just to fix problems, but to prepare for what’s next.”

– Channel partner respondent

A collaborative business partner

What was once a cost center is becoming a proactive value driver. Physical security is increasingly contributing to the achievement of organizational goals by providing actionable insights that support business continuity and innovation. Security data is also being recognized as a key resource for improving efficiency and decision-making.

This demand for greater value from security systems has led physical security teams to collaborate with other departments. Respondents expected greater integration in 2025 between building automation, visitor management, and other enterprise applications:

24%

of end users responded that they collaborated with other departments in 2025 for other business outcomes.

14%

of end users responded that they collaborated with other departments in 2025 for visitor management.

11%

of end users responded that they collaborated with other departments in 2025 for Industrial IoT.

10%

of end users reported that they collaborated with other departments in 2025 for occupancy management.

“Our focus is on transforming security from a reactive cost center into a proactive enabler for organizations. Strong collaboration between integrators, manufacturers, and clients will be essential to achieve this vision.”

– Manufacturer respondent

IT's growing presence in physical security

IT is embedded in the physical security conversation. The increasing sophistication of physical security operations has compelled the industry to evaluate new, innovative software and hardware. As physical security intersects with other departments and generates mission-critical data, IT has become an active participant in the industry's technology evolution.

Ranking the buying group

Findings show that IT departments are playing a larger role in physical security purchasing decisions. End users see executive leadership, finance, and IT as the most influential groups, underscoring how budget approval drives the process. Channel partners, on the other hand, place more weight on technical decision-makers.

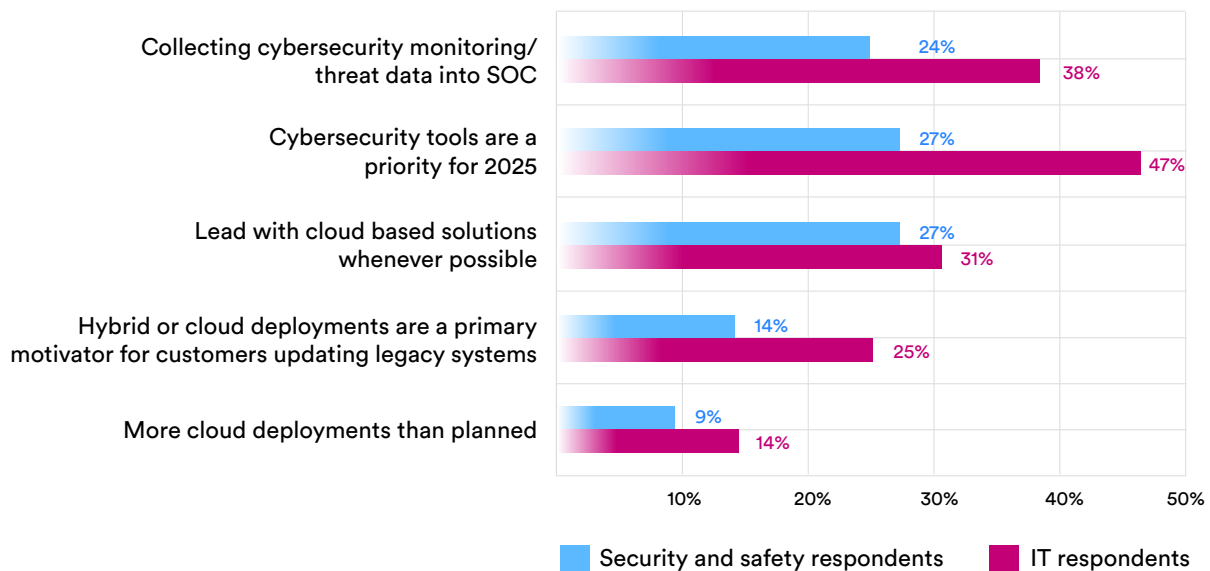
Top departments involved in the purchasing decision

	End users	Systems integrators	Consultants
Business operations (e.g. production managers, logistics, business analysts, data scientists, marketing)	5	-	-
Physical security department	4	2	1
IT department	3	1	2
Accounting and finance department	2	-	5
Executive leadership (e.g. president, chief executive officer, chief operating officer)	1	5	4
Security operations department	-	3	3
Procurement department	-	4	-

The transformative effects of IT's role

Collaboration between IT and physical security strengthens resilience by uniting cyber and physical defenses, streamlining processes, and sharing data. It also speeds the adoption of new technology, positioning physical security as a true business enabler.

Physical security versus IT respondents



Survey data reiterates that IT expertise supports modernization and ensures systems are deployed securely and effectively. This is seen in IT respondents' priorities for 2025:

47%

of IT respondents identified cybersecurity tools as a top priority, compared with 27% of physical security respondents.

38%

of IT teams collect cybersecurity data in their SOC, compared with 24% of physical security teams.

31%

of IT respondents said they lead with cloud-based solutions whenever possible, versus 27% of physical security respondents.

While IT teams appear ahead in aggregating cybersecurity data, physical security is catching up with unified platforms and shared data.

The digital revolution of security operations

“I see increasing demand for unified platforms that combine physical security, cybersecurity, and business intelligence. Customers want solutions that not only protect assets but also provide measurable ROI and integrate seamlessly with broader enterprise systems.”

– Channel partner respondent

For many, a change of pace means breaking down IT silos. Interdepartmental collaboration encourages more agile technology adoption, especially in areas like cybersecurity, shared network infrastructure, policies, and analytics.

Physical security is entering a new digital phase. Survey findings show that technology is reshaping the industry by connecting devices, data, and decision-making in ways that reach beyond traditional operations. Over the past two decades, IP technology has laid the foundation. Now, cloud capabilities are accelerating adoption and expanding what's possible.

By harnessing cloud processing, AI, and data sources, physical security is evolving from protection to insight, turning real-time information into faster responses and better decisions.

To sustain progress, security leaders must align IT and security teams around shared infrastructure and data. This will propel technology adoption, build stronger network resilience, and support a freer flow of information across the organization.

Where unification meets cyber risk

The boundary between digital and physical threats is disappearing. Findings indicate that, as physical security systems become more connected, safeguarding IoT and edge devices is now a core operational requirement.

This year's results also indicate that the adoption of cybersecurity tools is rising steadily as organizations modernize their environments. The data indicates stronger investment in prevention tools and more proactive project planning across all organization sizes:

34%

of end users have already deployed cybersecurity tools (up from 32% in 2024).

37%

of respondents plan to launch new cybersecurity projects in 2026 (up from 24% in the previous survey).

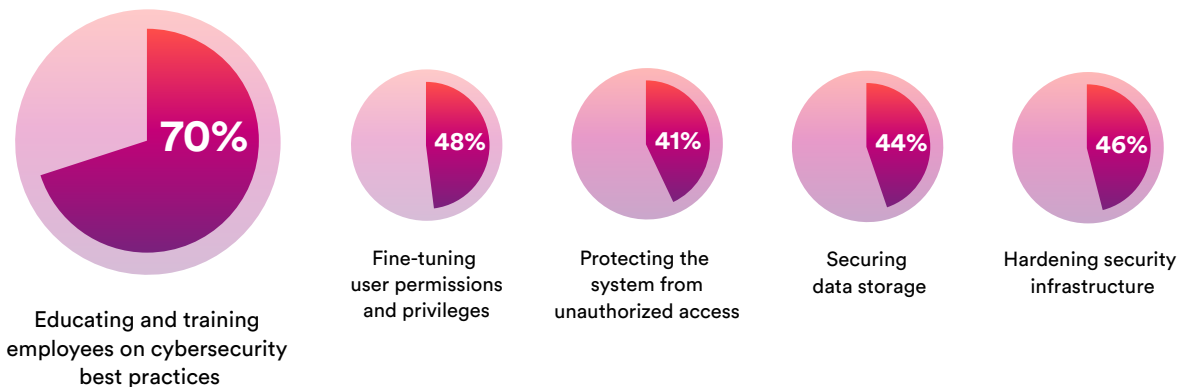
37%

of respondents reported an increase in physical and/or cybersecurity incidents in 2025.

48%

of large organizations, 10,000+ employees, reported an increase in physical and/or cybersecurity incidents in 2025.

When it comes to cybersecurity, what specifications/ approaches has your organization taken?

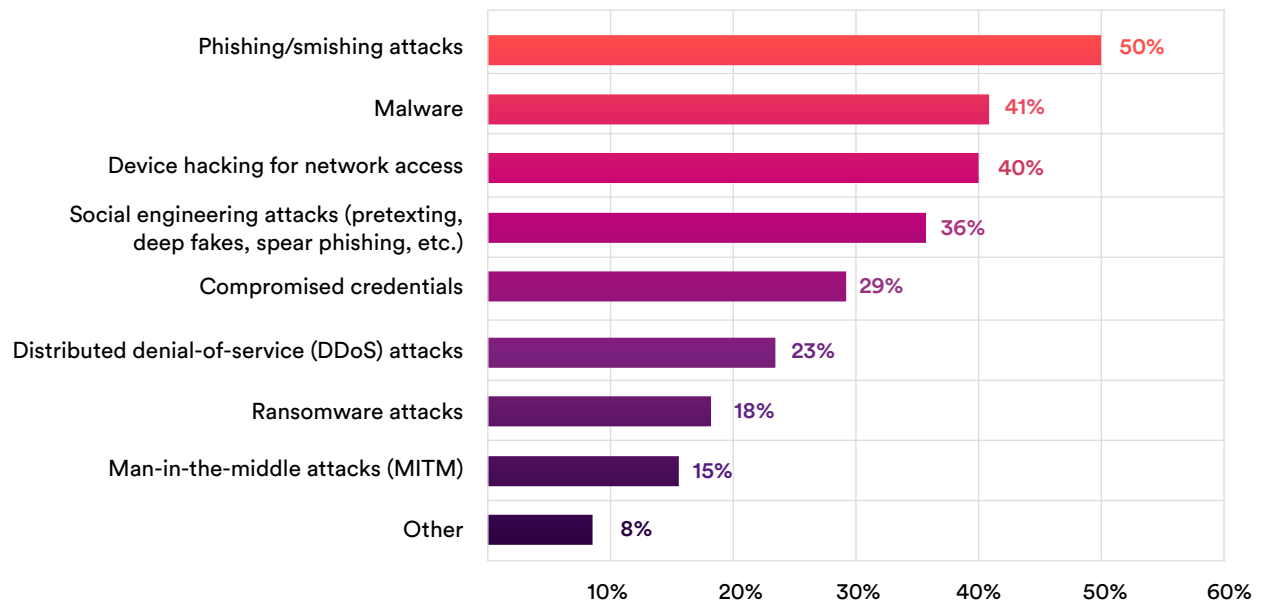


MULTIPLE RESPONSES ALLOWED; PERCENTAGES REFLECT SHARE OF END USER RESPONDENTS SELECTING EACH OPTION.

People-focused defenses are central to organizations' approaches, while technical measures also continue to support overall security.

With cybersecurity incidents on the rise and physical security systems more connected than ever, collaboration with IT is not just beneficial but essential. Physical security operations must continue to evolve to protect networks, as well as people and property.

What increases in cybersecurity incidents did your organization experience in 2025?



MULTIPLE RESPONSES ALLOWED; PERCENTAGES REFLECT SHARE OF END USER RESPONDENTS SELECTING EACH OPTION.

Insight

47% of IT end users identified cybersecurity tools as a priority for 2025 (versus an average of 37% of all respondents).

Compliance as a measure of maturity

As industries mature, regulations follow close behind. These often concern standardization, risk management, trust, and compliance. Survey results found this was true for physical security, especially now that security teams are partnering more with IT. These frameworks ensure that the right systems are installed, maintained, and operated to protect both physical and digital assets.

Only 16% of end users said their organizations had been directly affected by industry or government compliance requirements (21% among IT respondents) versus 40% by channel partners and manufacturers. These differences show that compliance efforts are often led by suppliers (manufacturers, integrators, and IT specialists), who generally face regulatory pressure first. They are responsible for ensuring products and systems meet standards before reaching the end user.

“Our clients have been impacted by regulations... and have been driven to strengthen cyber resilience [to] improve the storage and protection of sensitive data.”

– Consultant respondent

Channel partners and manufacturers reported that regulatory and governance requirements are influencing purchasing decisions and system upgrades:

40%

said compliance is now a primary motivation for replacing legacy systems.

End users whose organizations have been affected by industry regulations or compliance



The cloud as an enabling force

Cloud infrastructure is powering technology evolution at scale, and the physical security industry is no exception. Cloud appliances and edge devices are transforming how security is deployed and maintained. These components simplify connectivity across multiple applications and sites, support easier scaling, and improve agility through automatic software updates, remote diagnostics, and reduced technician visits.

End users’ top 5 most important reasons for adopting cloud in physical security

	2024		2025
Automatic system updates and new features	1	→	1
Ease of deployment	3	↑	2
Easier to maintain systems/servers across the network	2	↓	3
Ability to outsource monitoring and maintenance	4	→	4
Easier to scale the system	5	→	5

AUTOMATIC UPDATES AND EASE OF DEPLOYMENT CONTINUE TO LEAD CLOUD ADOPTION PRIORITIES.

“We are looking to improve collaboration between different offices and departments, as well as the possibility of easily integrating new technologies and systems.”

– End user respondent

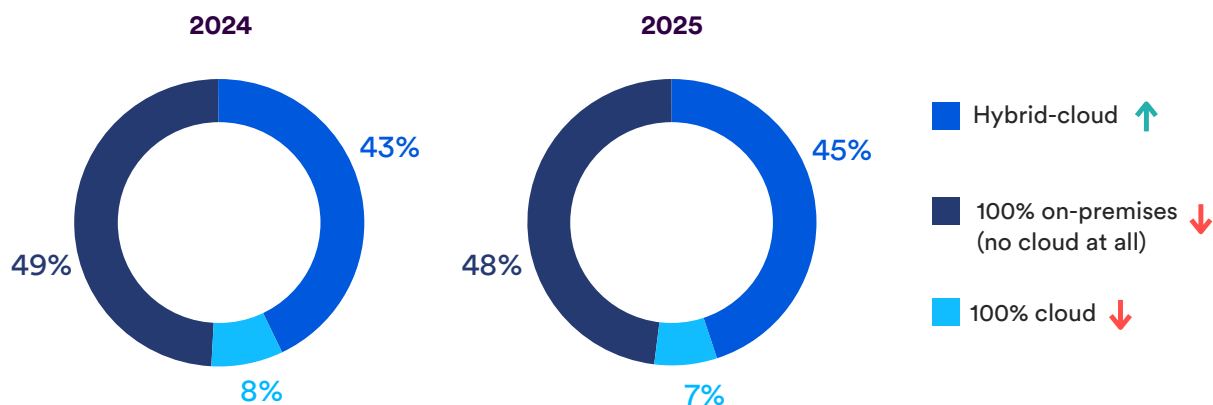
Achieving versatility with cloud and hybrid-cloud

Organizations are looking to maximize flexibility and performance. Survey findings suggest that respondents understand they don't need to be confined to a cloud-only deployment. Instead, they have the freedom to choose the approach that fits their operational needs.

According to the results, users are settling into defined cloud strategies, favoring hybrid models that balance

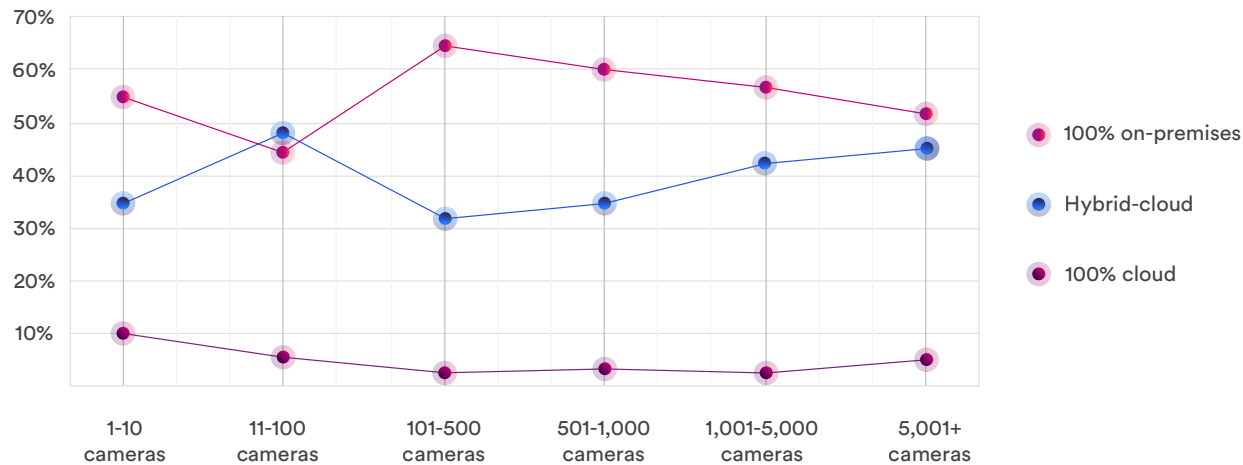
scalability with the flexibility to keep specific workloads on-premises when needed. This includes partitioning systems into distinct security zones² to ensure that critical functions remain operational even during cloud disruptions. Doing this enhances resilience, continuity, and control across both cloud-connected and local systems.

How much of your physical security environment is cloud or hybrid-cloud?



2. Security zone: independently managed areas within the physical security infrastructure that can operate autonomously.

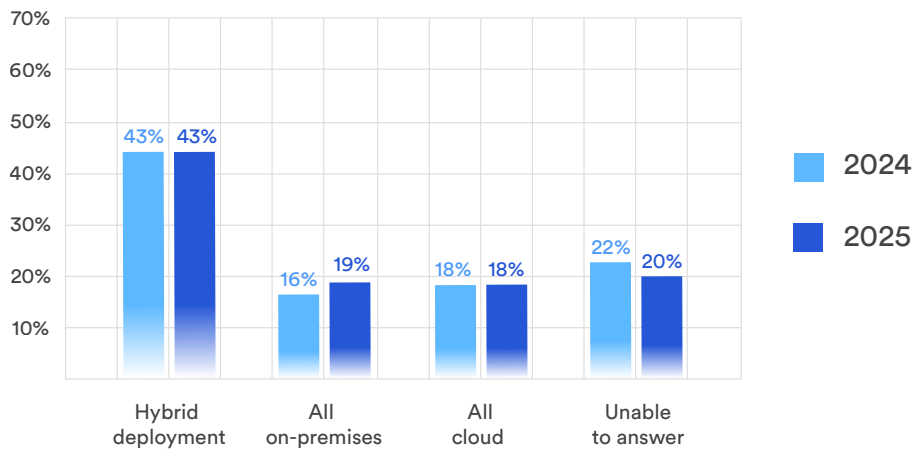
How much of your physical security environment is cloud or hybrid-cloud?



BY END USER ORGANIZATION CAMERA COUNT.

In the years to come, end users are planning to continue their transition to the cloud, and most are prioritizing hybrid deployment models:

Over the next 5 years, what is your company’s target vision for security deployment in the cloud?



A sunny outlook for cloud adoption

Cloud growth is signaling confidence in modern, connected technology. Manufacturers, channel partners, and consultants anticipate that end users will have continued interest in moving parts of their security infrastructure to the cloud.

While some end user hesitancy remains due to concerns over data loss, pricing, ownership costs, and vendor lock-in, physical security practitioners are trending toward incremental cloud adoption aligned with business needs.

61%



of consultants expect their customers to shift some workloads to the cloud within the next 12 months (up from 58% previously).

72%



of consultants say they plan to specify hybrid deployments over the next five years, signaling a pragmatic, hybrid-first transition.

Insight

71% of channel partner respondents expect new cloud system deployments in 2026, while only 3% anticipate any decline in adoption.

“Cloud or on-prem, or a mix of both? The right deployment depends on your organization’s size, security environment, and priorities.

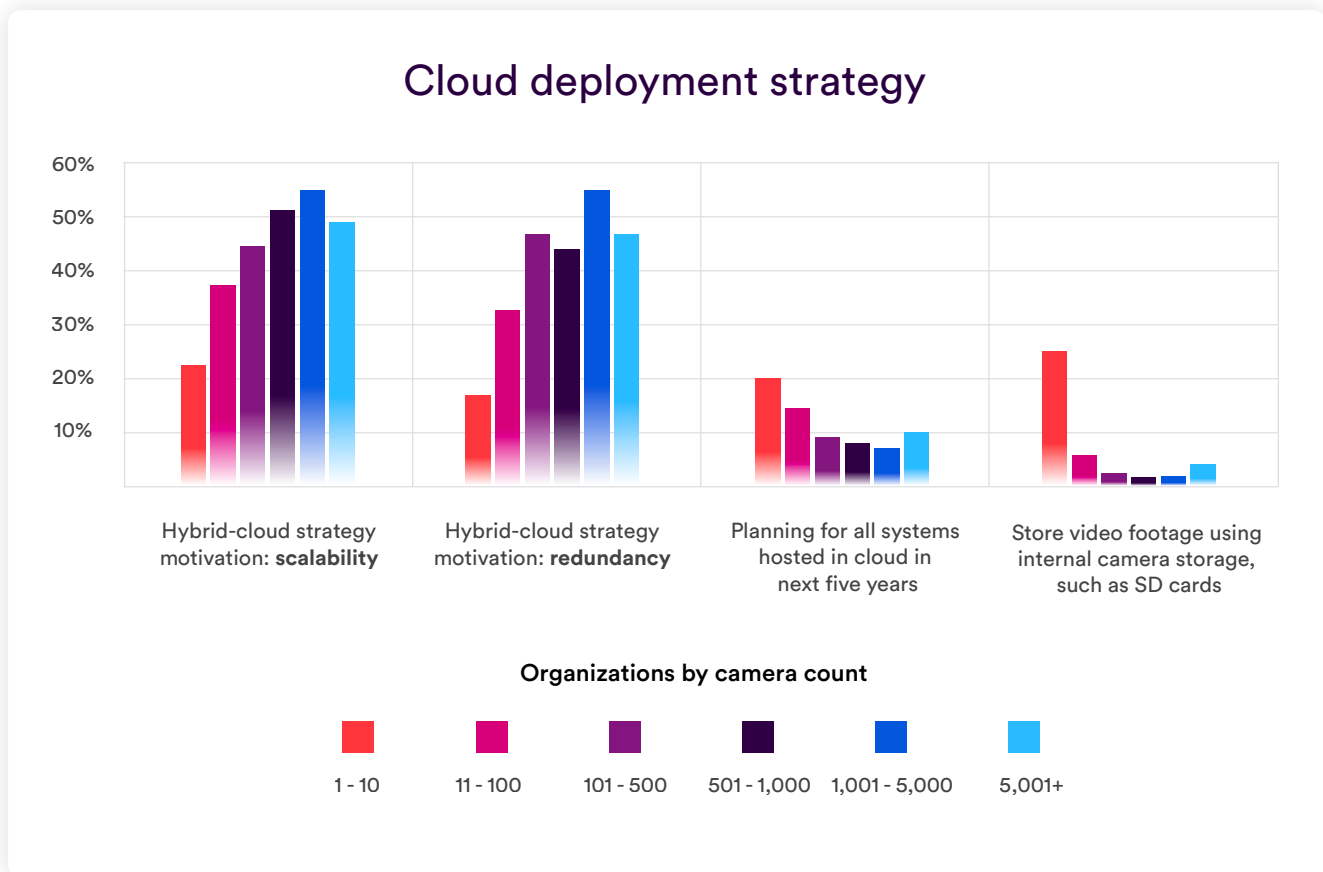
That’s why deployment choice matters.”

Despina Stamatelos

Director, Product
and Industry Marketing
Genetec Inc.



According to survey data, adoption strategies also vary by system scale:



BY END USER ORGANIZATION CAMERA COUNT.

Large organizations are less likely to depend on on-camera storage (SD cards) and are unlikely to adopt full cloud hosting within the next five years. Redundancy and scalability continue to be the strongest

drivers for large organizations to choose hybrid models, where cloud appliances help bridge on-premises infrastructure with cloud services, supporting reliable performance across complex environments.

Growing momentum for access control in the cloud

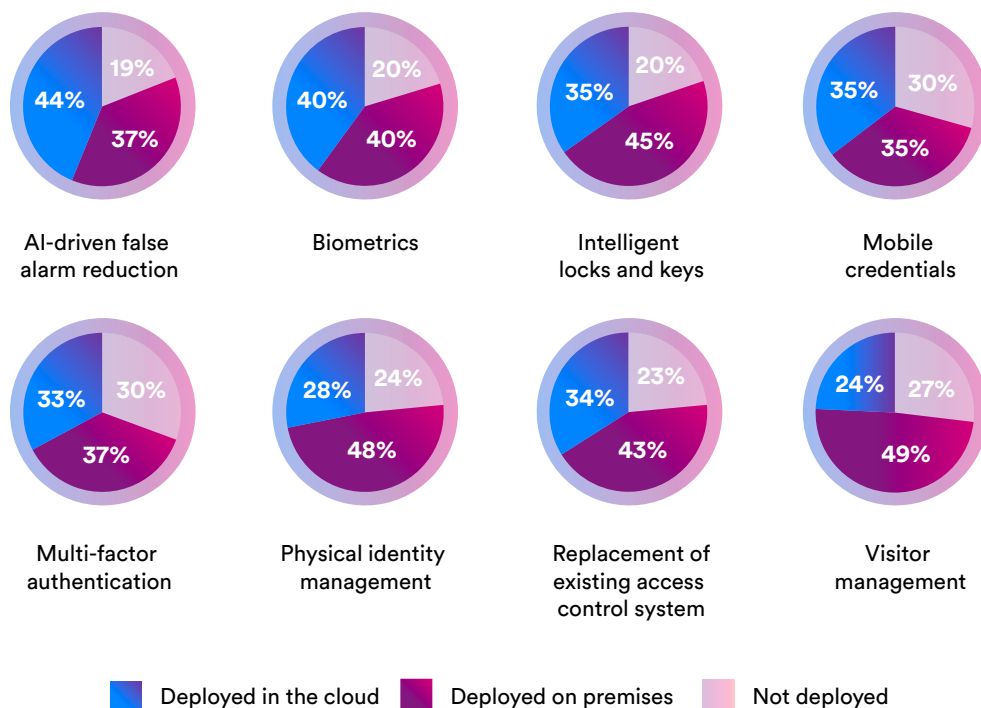
Access control as a service (ACaaS) is beginning to gain ground

This is due to its deployment ease and lighter data requirements, minimal cloud setup, and straightforward hardware needs. Among respondents, 11% of end users indicated full deployment of their access control system in the cloud, while 27% operated hybrid systems.

Planned access control capabilities for 2026

Survey responses suggest that organizations are prioritizing scalability and modernization as they expand access control functionality. The demand for AI-driven alarms, multi-factor authentication, and mobile credentials is helping fuel the rise of ACaaS deployments:

What capabilities do you plan to add to your access control system in 2026?



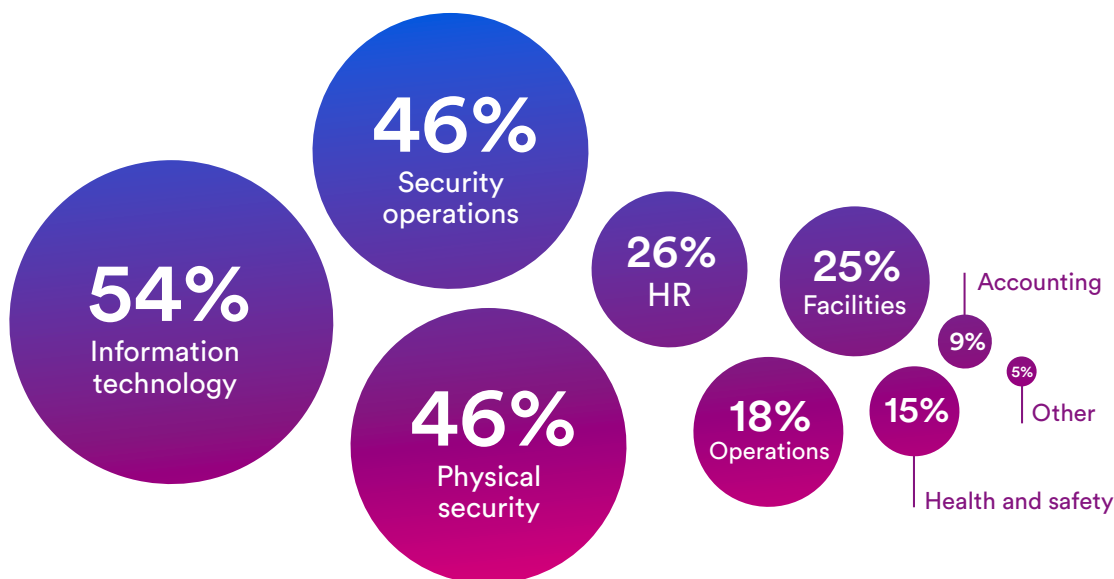
END USER RESPONSES ONLY.

Physical security data: A shared asset

Physical security departments serve as custodians of extensive data across a wide array of systems and sensors. This data underpins operational intelligence for both security operations and organizations as a whole. As security systems mature, data is facilitating smarter, more connected operations.

While IT teams have always understood and managed the value of this strategic resource, physical security is starting to recognize the importance of sharing and receiving data. Survey findings reveal that 25% of end users share data with and receive data from other departments.

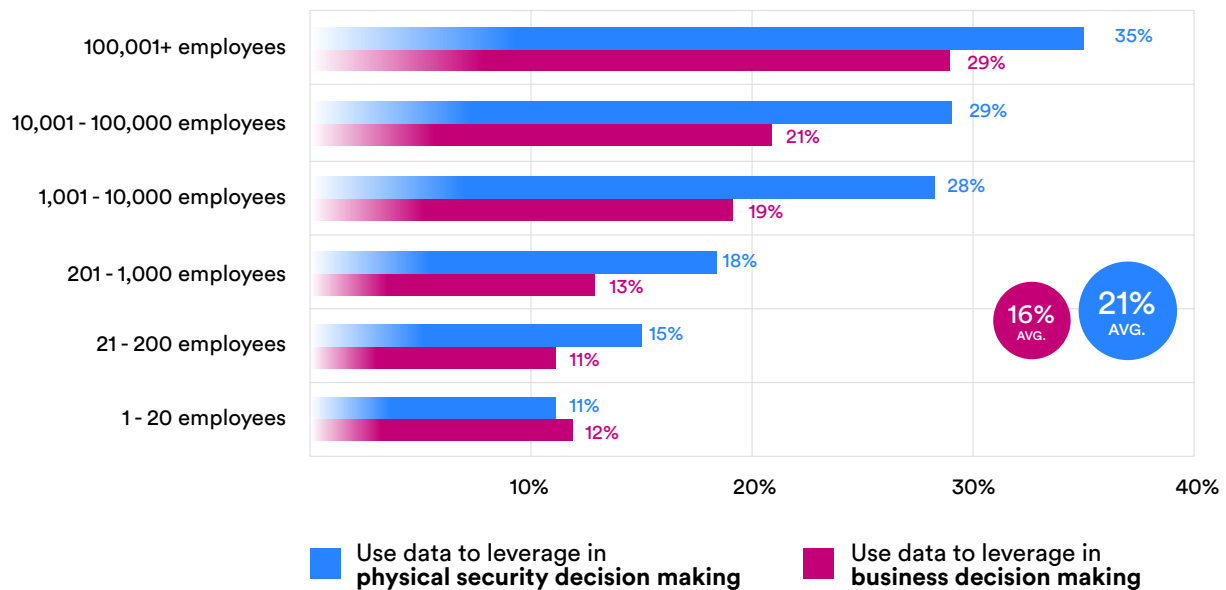
What departments receive physical security data in your organization?



MULTIPLE RESPONSES ALLOWED; PERCENTAGES REFLECT SHARE OF END USER RESPONDENTS SELECTING EACH OPTION.

Large organizations are leading the shift toward data-driven security:

What are the core functions of your physical security operations?



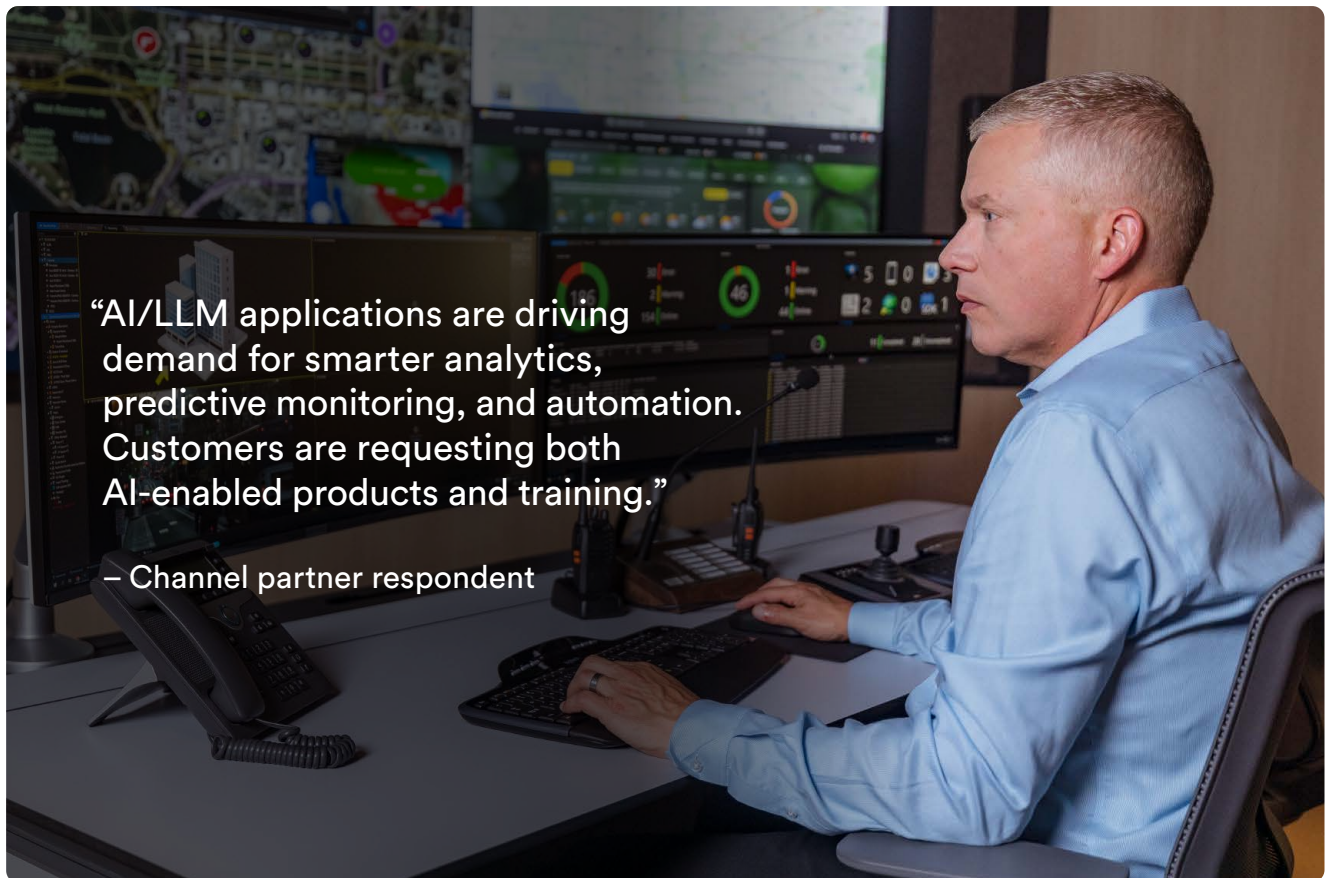
END USER RESPONSES ONLY.

It's no surprise that large enterprises, with their robust systems and staff, are most likely to use physical security data. However, data use is common across organizations of all sizes. This highlights how data is repositioning security from a budget line item to a driver of efficiency, insight, and resilience.

AI and analytics: From sensing to sense-making

Artificial intelligence (AI) expectations are all over the map. AI can make physical security more effective at detecting anomalies, anticipating incidents, and enabling faster, more confident decision-making when

the technology is implemented properly. But realizing this potential requires connected systems and the elimination of barriers to data-sharing.



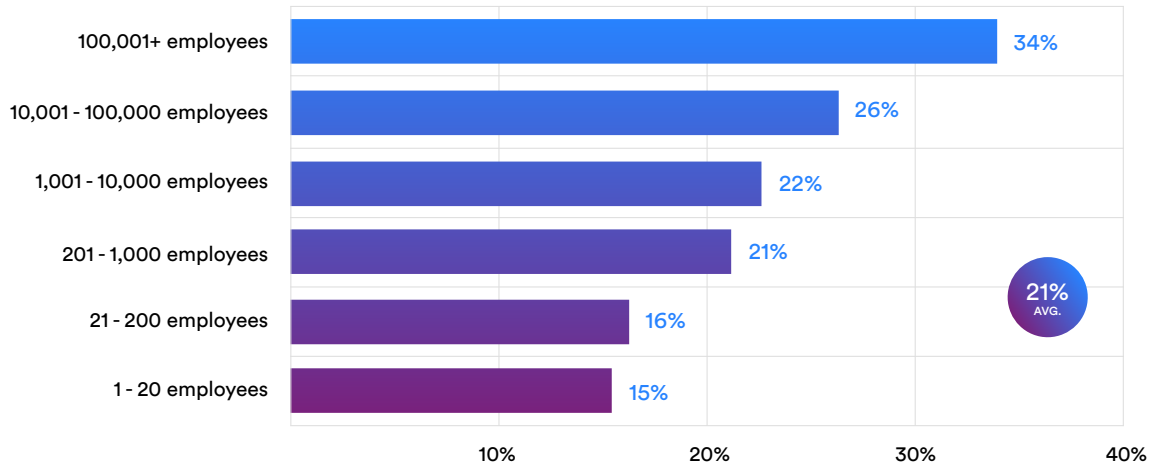
“AI/LLM applications are driving demand for smarter analytics, predictive monitoring, and automation. Customers are requesting both AI-enabled products and training.”

– Channel partner respondent

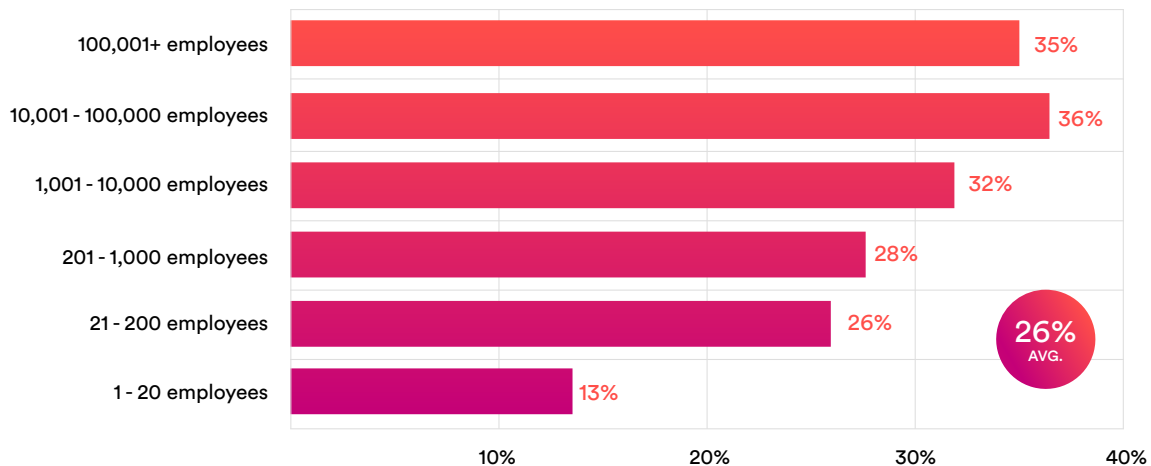
LLM: LARGE LANGUAGE MODEL

Technology currently deployed in end users' physical security environments by total employees

AI and/or LLM



Data analysis and visualization tools

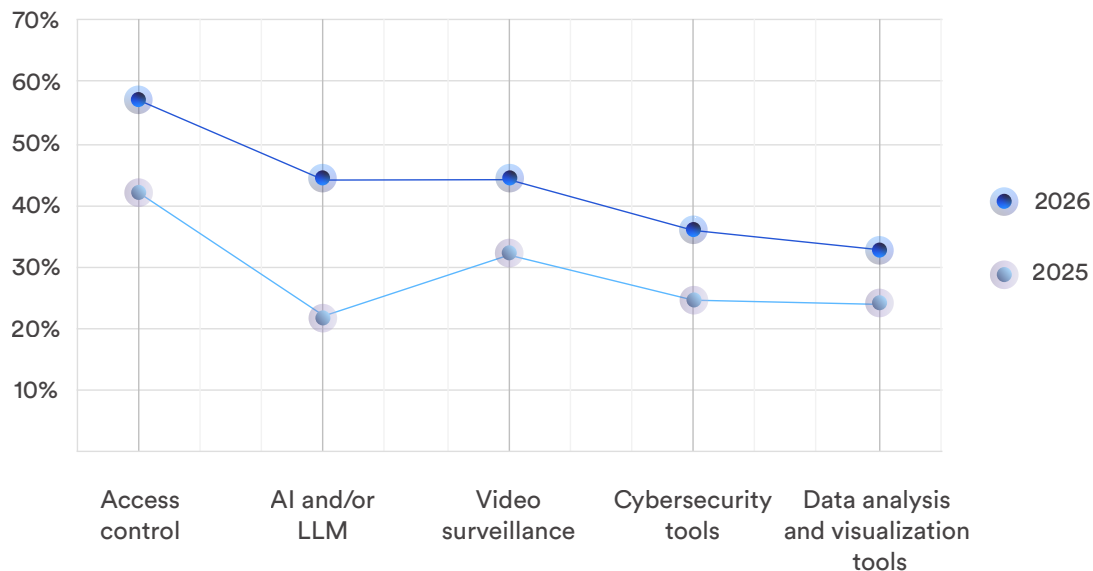


Some organizations are already advancing their adoption of AI and data visualization tools. Survey results show that large organizations are experimenting more and leading this shift, supported by bigger budgets and larger IT and physical security teams. For these companies, it's more feasible to embrace and adopt these innovations.

All eyes on AI in the year ahead

AI is a preoccupation for physical security. For the first time, AI ranked alongside access control and video surveillance as a key priority for 2026.

What type of project will be the focus of your department for next year?



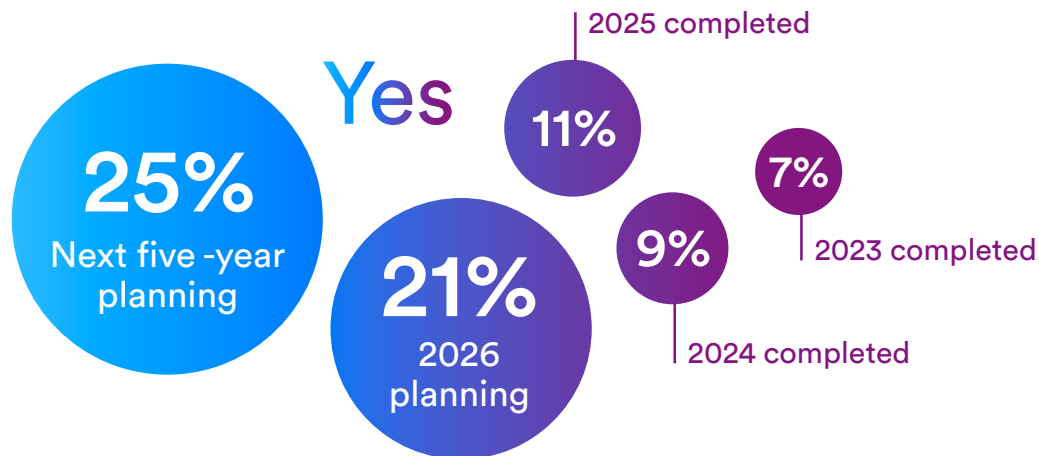
As adoption and interest grow, the pressure is on channel partners and manufacturers to deliver AI solutions that meet user needs. End users are focused on where they can find value, but many need support to find a way to benefit from AI-based technology.

Survey findings reveal that end users see value in systems that leverage AI to improve security operations by helping operators navigate alarms and investigations, reducing noise, and prioritizing the events that matter.

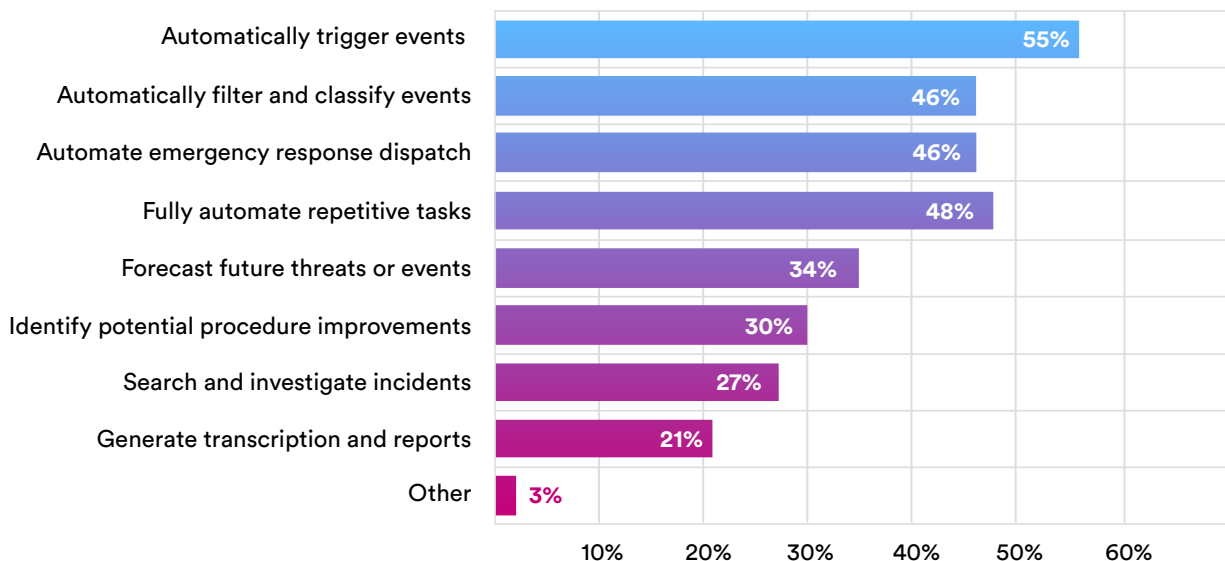
However, no single solution stands out. End users still need guidance, not only in choosing the right products but in understanding how AI can translate into real-world impact.

Systems integrators and manufacturers will need to collaborate closely with end users, innovate responsibly, and manage expectations to deliver meaningful, measurable outcomes with this technology.

Is your organization planning to integrate machine learning, AI, and/or LLM applications in your environment?



What is your organization trying to achieve by integrating AI?



MULTIPLE RESPONSES ALLOWED; PERCENTAGES REFLECT SHARE OF END USER RESPONDENTS SELECTING EACH OPTION.

Top concerns about implementing AI in physical security

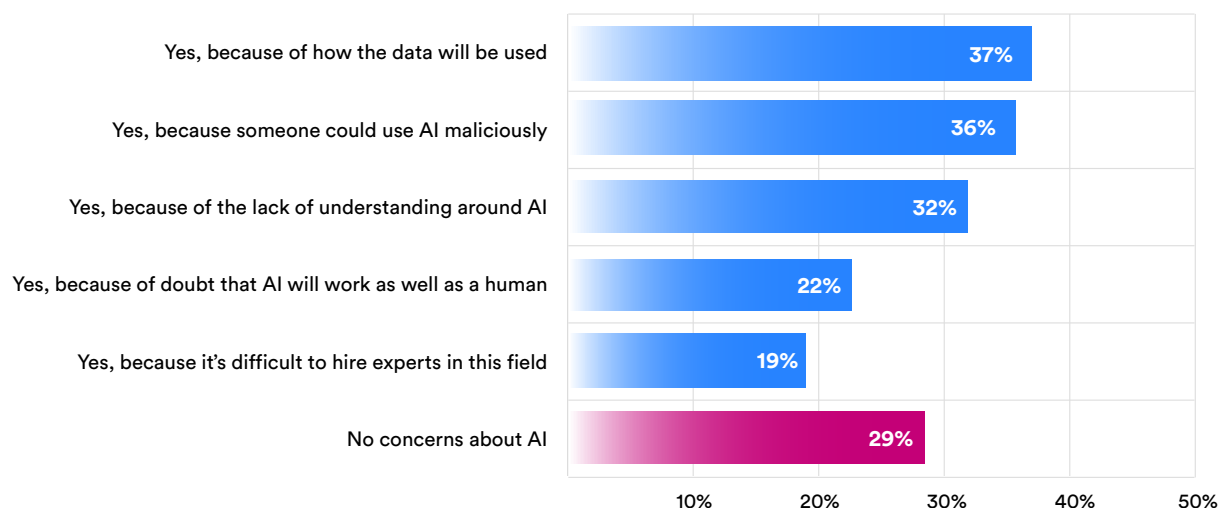
“[We have] concerns about auditability and regulatory defensibility. AI decisions—especially in surveillance and access control—must be explainable and auditable to satisfy compliance audits and legal scrutiny.”

– End user respondent

Confidence in AI is growing, but unease over implementation persists. Only 29% of end user respondents stated they have no concerns about AI. Meanwhile, 70% of end user respondents are worried about how

AI systems are designed and implemented. They have specific concerns about how the data will be used and about not understanding the technology.

Are there concerns within your organization about implementing AI technology?



MULTIPLE RESPONSES ALLOWED; PERCENTAGES REFLECT SHARE OF RESPONDENTS SELECTING EACH OPTION.

“End users depend on us to turn innovation into practical tools that improve their operations. That’s why we focus on choosing the right technology for the right challenge.

AI is no different. It takes time, creativity, and responsible development to make it truly useful.”

Anne-Cécile Tournier

Product Group Director,
Intelligent Automation
Genetec Inc.



The 2026 forecast

Changing market dynamics

Surveyed channel partners and manufacturers identified several key challenges that could affect budgets and project timelines in 2026. The primary drivers included economic pressures, such as tariffs, inflation, rising costs, and supply chain disruptions.

Respondents also expressed concern that these persistent challenges may stretch available resources and lead to delays in obtaining hardware and essential components.

What do you expect could cause project delays next year?



MULTIPLE RESPONSES ALLOWED; PERCENTAGES REFLECT SHARE OF CHANNEL PARTNER RESPONDENTS SELECTING EACH OPTION.

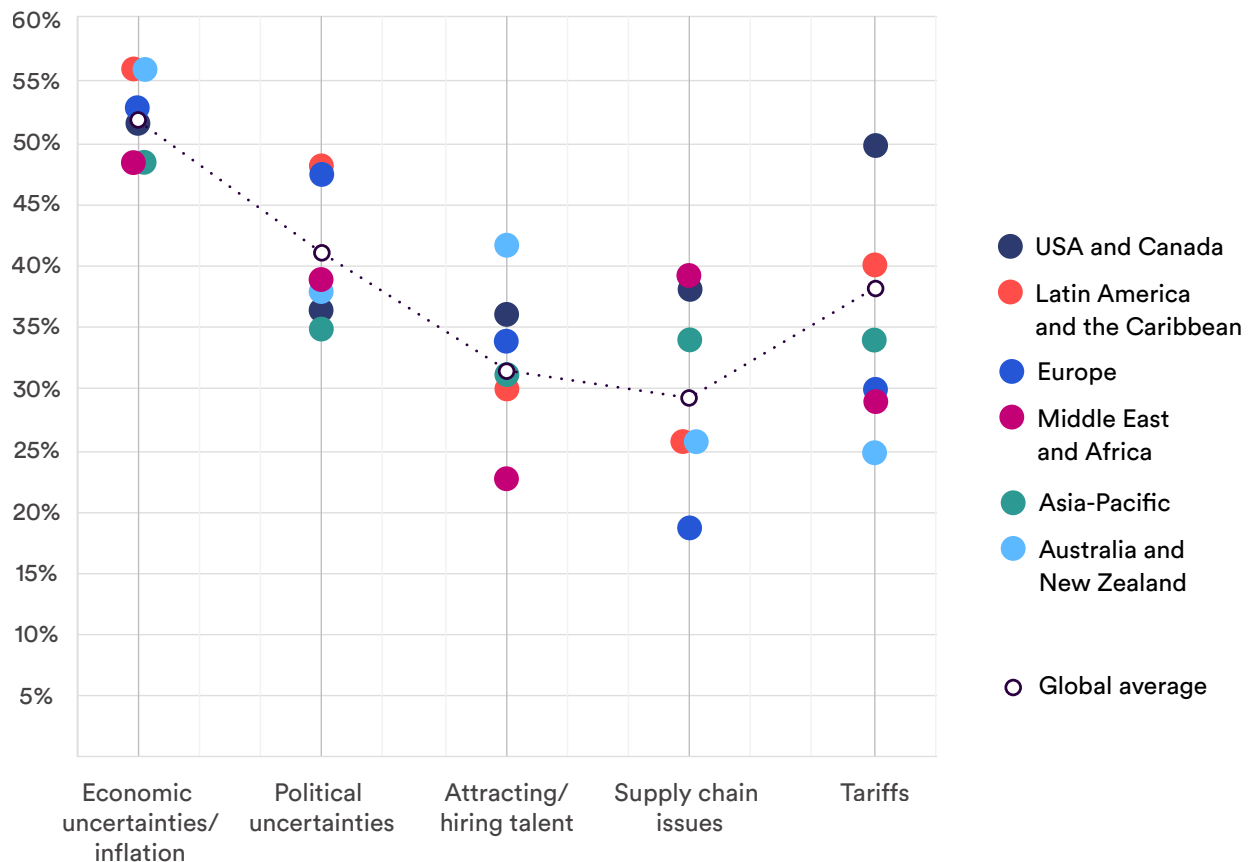
When considering regional differences, economic uncertainty and inflation emerged as the most pressing concerns. While tariffs and supply chain disruptions were also widely mentioned, their potential impact varied depending on geographic differences.

Political instability was considered a moderate concern overall, but channel partners and manufacturers in North America demonstrated greater sensitivity to this issue.

Supply chain issues were identified as a higher risk in the Middle East and Africa and Asia-Pacific regions compared to other regions.

The results clearly indicate that while economic pressures are a global concern, their effect on the physical security sector differs by region.

Top 5 expected reasons for project delays in 2026

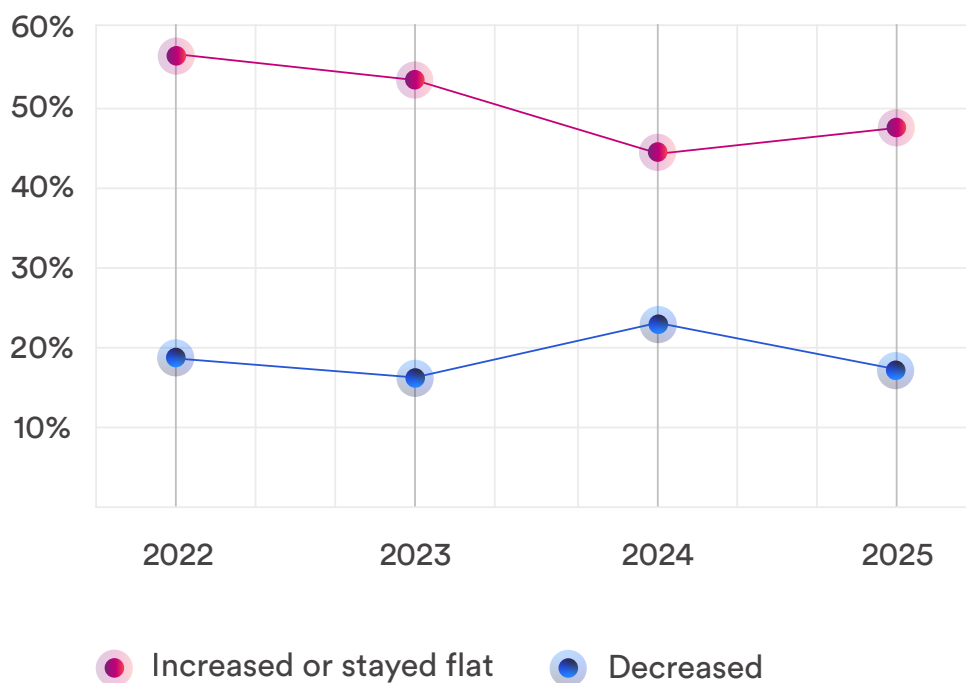


CHANNEL PARTNER RESPONSES ONLY.

Proof of optimism: The outlook on 2026 budgets

Uncertainty marked 2025, but spending held steady. Among end users, 48% reported that their 2025 operational budgets either increased or remained stable. Year-over-year results from the State of Physical Security report demonstrate this budget resilience, spotlighting the industry's enduring strength and adaptability.

Reported changes to end user OpEx budgets



END USER RESPONSES ONLY.

Data also supports optimism going into 2026, as the mission-critical role of safety and security evolves beyond its traditional boundaries into

a business enabler. Industry analysts also predict solid growth³, and 58% of consultants expect their customers' budgets to remain steady or increase.

3. Industry analyst research – (1) Novaira Insights – World market for video surveillance hardware and software – 2025: In the global video surveillance market (excluding China), hardware revenue is projected to grow at 7.4% CAGR, and software/services are forecasted to expand even faster at 12.1% CAGR between 2024 and 2029. (2) Omdia & SIA-ASIS (2024) - Complexities in the global security market: 2024–2026: The physical security equipment market is projected to grow from \$60.1 billion in 2024 to \$70 billion by 2026, reflecting an 8.2% CAGR, while security services are expected to reach \$389 billion by 2026.

The economic landscape's impact on staffing

A tightening labor market is changing how the industry builds and retains talent. As digital transformation gains ground, the demand for skilled talent continues to exceed supply. Findings show clear regional differences in workforce priorities:

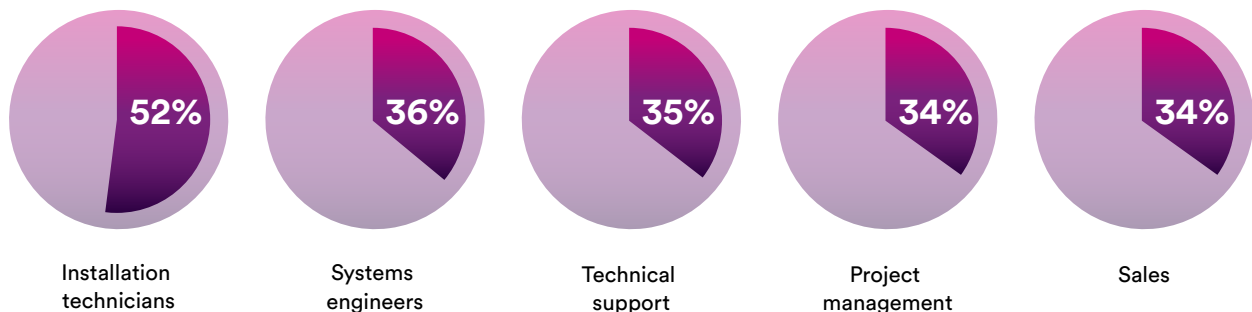
- Attracting and hiring talent was raised as a key challenge in North America, Latin America, and Asia-Pacific
- Training and upskilling talent was emphasized as a challenge by respondents in North America, Europe, and Australia and New Zealand
- Managing a remote workforce was reported as an ongoing issue across all regions

A global shortage of skilled technical professionals is causing project delays and making it more difficult and time-consuming for organizations to train staff on emerging technologies.

“There is a surge in demand for technicians and engineers who are proficient in cloud computing, IoT, and AI. Demand is outpacing the supply of suitably skilled personnel.”

– Channel partner respondent

Which departments gave you staffing challenges?



CHANNEL PARTNER RESPONSES ONLY.

To address these challenges, channel partners and manufacturers are taking a new and more strategic approach to workforce needs:



Investing in training, cross-skilling, and up-skilling

Enhancing staff capabilities through structured technical programs and cross-functional skill development



Adopting a skills-first approach

Focusing on technical proficiency and adaptability over traditional roles



Leveraging AI for process optimization

Automating workflows to boost efficiency, not just reduce headcount



Integrating IT optimization talent

Recruiting ERP, WMS, and IT professionals to bring an optimization-first mindset



Supporting employee well-being

Investing in workplace flexibility and wellness to improve retention; managing remote work requests

End users also voiced concerns about staffing shortages, reliability of vendor support, and slower project deployments. As technology adoption advances, limited technical expertise could create more deployment

challenges. At the same time, new AI solutions with intelligent automation and intuitive interfaces may help ease some of these pressures by making systems easier to use and manage.

Insight

The share of channel partners and manufacturers expecting hiring delays dropped from 44% to 32% in 2025—an encouraging sign, even as 97% still anticipate staffing challenges will persist or worsen in 2026.

Heading into 2026, the industry's main challenge is more than just filling open positions. It lies in enabling HR teams to keep pace with ongoing transformations across physical security.

Success will depend on collaboration among manufacturers, systems integrators, and end users, along with sustained investment in training to ensure new hires stay up to date with the latest innovations.



“... AI and cloud computing are evolving rapidly ... even if employees receive initial training on new technologies, they might quickly fall behind without continuous learning.”

– Channel partner respondent

Adapting project priorities for 2026

Core systems remain the backbone of physical security, but priorities are changing. Survey results show that while access control and video surveillance continue to anchor operations, new initiatives are redefining how organizations approach their security needs. Here is how end users responded:

Access control

58%

marked this as their top priority, reflecting a strong push to update systems and activate new capabilities.

AI and LLM

44%

said they are prioritizing these tools for enhanced analytics and automation.

Video surveillance

43%

confirmed video remains central to both security operations and organizational intelligence.

Cybersecurity tools

36%

are focusing on strengthening network and system protection.

Data analysis/ visualization

33%

stress that they value tools that provide actionable insights.

Cross-department collaboration

31%

embrace integrated efforts with HR, facilities, supply chain, and risk teams.

The survey also highlights the differing priorities of IT and security and safety teams that match their unique responsibilities. IT remains focused on enabling technology and ensuring resilient infrastructure, while physical security teams are focused on operational control and incident preparedness and response. Despite these differences, the findings reveal a shared focus on core systems, such as access control and video surveillance, to protect people and property.

What type of project will be the focus in 2026?

	Information technology (IT)	Security and safety
Access control	1	1
Video surveillance	2	2
Cybersecurity tools	3	-
AI and/or LLM	4	3
Video analytics (business intelligence, privacy masking, or threat detection)	5	-
Incident management	-	4
Intrusion	-	5

END USER RESPONSES ONLY.

Other shared priorities include AI and video analytics, which can enable smarter threat detection, automate routine monitoring, and generate insights. These analytics improve operational efficiency, reduce response times, and support data-driven decision-making across the business.

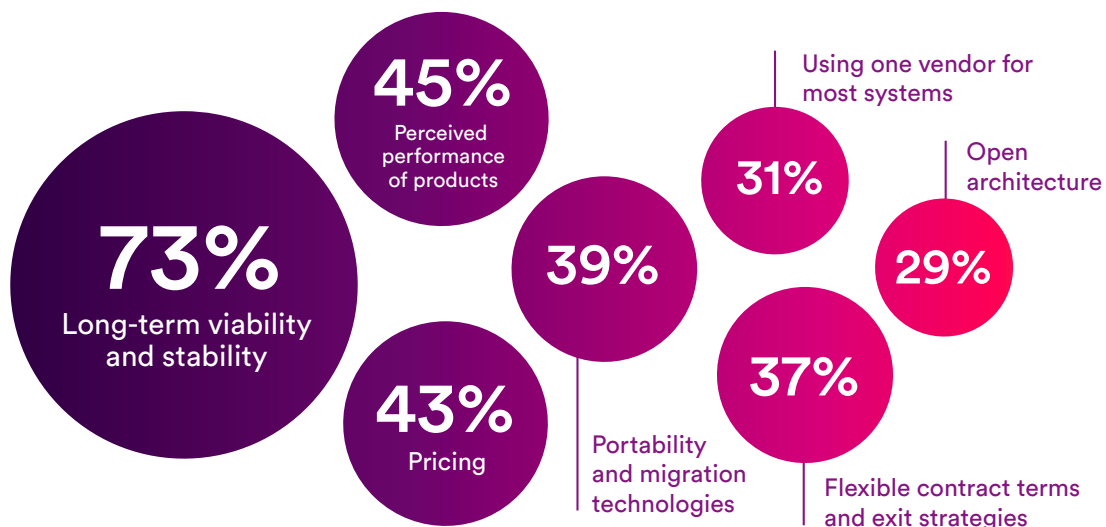
While IT and physical security teams have their own primary objectives, survey findings stress that they are on the same page. By combining technical expertise with physical security expertise, both teams are better equipped to address security challenges proactively.

From vendors to value partners

The physical security industry is undergoing a phase of accelerated innovation, fueled by advances in artificial intelligence, cloud computing, and the growing sophistication of how organizations operate. As these innovations reshape the industry, organizations are reevaluating their perspectives on systems integrators and manufacturers.

The survey data shows customers now place more value on long-term alignment and vendor stability. They expect partners to bring design and deployment expertise, deliver solutions that maximize value, and reduce total cost of ownership. End users also expect manufacturers to act responsibly and collaboratively and to offer practical, forward-looking solutions that meet their needs and position them for success.

When it comes to working with physical security vendors what are you looking for?



MULTIPLE RESPONSES ALLOWED; PERCENTAGES REFLECT SHARE OF END USER RESPONDENTS SELECTING EACH OPTION.

Key takeaway 1

Technology as a catalyst for progress

Traditionally focused on reliability and risk mitigation, the physical security industry has been cautious in adopting new capabilities. The pandemic marked a turning point, accelerating the adoption of cloud-based solutions to maintain operations and continuity.

Technology is now viewed as a strategic enabler that drives greater efficiency and agility in responding to emerging threats. Leaders are no longer debating innovation but deploying it to maximize long-term value and shape the industry's future. This generational change reflects the growing belief that new technologies are essential to protecting people and assets.

Embrace technology

The future belongs to those who use technology to make security smarter and more connected.

Key takeaway 2

Collaboration as an innovation driver

Closer alignment between IT and physical security teams is transforming how organizations solve problems and deploy technology. Progress now depends on shared expertise and mutual trust. Collaboration is no longer just about aligning technologies. It's about combining skill sets to solve problems in new ways and help organizations adapt quickly to shifting market demands and emerging threats.

The strength of this partnership lies in how physical security leaders gain new perspectives and rethink how technology can enhance, or even overhaul, traditional practices. Bringing together talent from diverse disciplines makes this possible, as effective security depends on blending technical expertise with human insight and ingenuity.

Transforming organizations

As the industry evolves, success will come from teams collaborating to turn technology into practical and effective solutions.

Key takeaway 3

Partnership as a measure of meaningful change

End users increasingly expect providers of physical security solutions to act as long-term collaborators rather than just suppliers. Systems integrators and manufacturers are now viewed as trusted partners who can facilitate meaningful change and protect technology investments over time. Expertise in both design and deployment, as well as an active commitment to responsible innovation, will define their success in a fast-shifting landscape.

End users also seek partners that demonstrate stability and insight, which can help them build enduring capabilities rather than chasing short-term technological trends. Longevity and total cost of ownership are top of mind as end users adopt and deploy new technologies. They seek solutions that deliver lasting value and partners who can help guide sound, long-term investments.

A shared vision

These partnerships will be instrumental in shaping the industry's future direction.

Appendix

Appendix 1 – Survey methodology

Genetec Inc. surveyed physical security professionals worldwide from August 18 to September 15, 2025. Following a review of submissions and data cleansing, 7,368 respondents were included in the sample for analysis.

Details about the survey and analysis

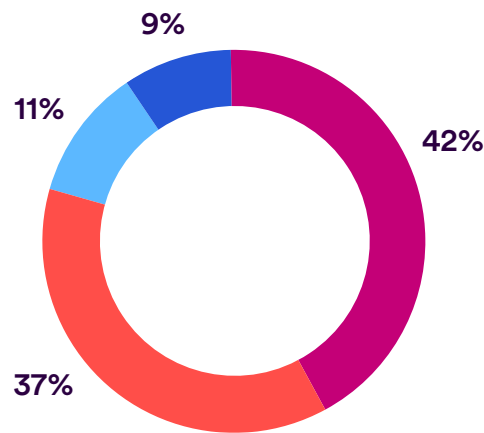
- The target population for the survey included individuals involved in the procurement, management, service, and/or use of physical security technology. Respondents represented Genetec end users as well as participants reached through in-person events, digital promotions, or opt-in email lists from third parties.
- Invitations were distributed via email in English, French, German, Italian, Japanese, Korean, and Spanish.
- The online survey form was available in English, French, German, Italian, Japanese, Korean, Spanish, and Portuguese.
- Only fully completed surveys submitted by individuals within the targeted population for the survey were included in the final analysis.
- Survey samples were run across all regions, including Asia-Pacific; Australia, New Zealand, and the rest of Oceania; Europe; Latin America and the Caribbean; the Middle East, Turkey, and Africa; and the USA and Canada.
- Response and completion rates varied by organization size, which may have introduced sampling variations or errors in sub-samples.
- Responses were collected from physical security end users, channel partners, manufacturers, and physical security consultants. Each target population was shown a slightly different set of questions reflecting their different perspectives.
- Data cleansing was performed to validate respondent classification into one of these four populations and limit potential errors. Any non-sampling errors are assumed to result from the collection of data from respondents outside the target population (for example, individuals incorrectly identifying themselves as end users when in fact they are employed as systems integrators).

A note about survey calculations

Due to rounding and survey design (including rating scale, select-all-that-apply, and multiple-choice questions), not all percentage totals in this report will equal 100%. For select-all-that-apply questions, which allowed respondents to choose multiple answers, percentages refer to the proportion of respondents who selected the individual answer.

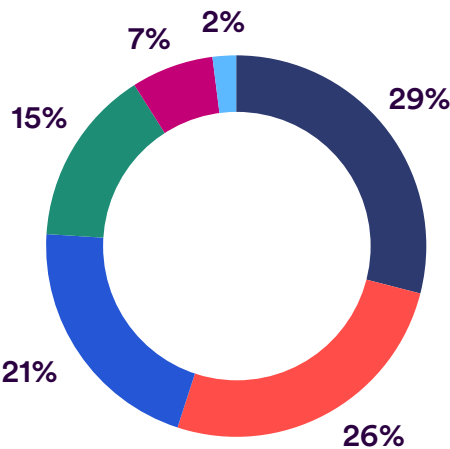
Appendix 2 – Respondent information

Respondent type
(7,368 respondents)



	Channel partners	42%
	End users	37%
	Consultants	11%
	Manufacturers	9%

Geographic region



	USA and Canada	29%
	Latin America and the Caribbean	26%
	Europe	21%
	Asia-Pacific	15%
	Middle East and Africa	7%
	Australia and New Zealand	2%

Appendix 3 – Respondent demographics

Job functions

Security and safety	12%
Information technology (IT)	12%
Sales	13%
Engineering, R&D, system design, and quality assurance	13%
Administration or office administration	5%
Customer service or support (technical support)	6%
Operations management	5%
Facilities or operations management	4%
Project management/risk or compliance management	5%
Accounting and finance	3%
Marketing	2%
Purchasing and procurement	2%
Legal	1%

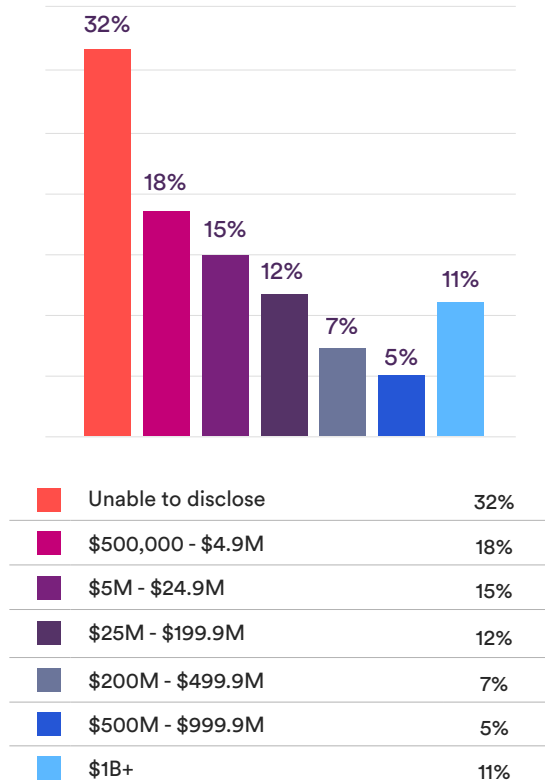
END USER RESPONDENTS BY JOB FUNCTION.

Industries

Industrial and manufacturing	13%
Education	12%
Banking and finance	10%
Transportation	10%
Energy, utilities, and telecoms	9%
Professional services and associations	8%
Federal or national government	8%
Sports, gaming, and hospitality	6%
Healthcare	6%
Retail	5%
Other	4%
Emergency services, justice, and public safety	4%
State or local government	3%
Traffic and parking	1%

END USER RESPONDENTS BY SECTOR.

Revenues



END USER RESPONDENTS BY THEIR ORGANIZATION'S TOTAL REVENUES (USD).

Employee count

1 - 20	20%
21 - 200	30%
201 - 1,000	20%
1,001 - 10,000	18%
10,001+	13%

END USER RESPONDENTS BY THEIR ORGANIZATION'S NUMBER OF TOTAL EMPLOYEES.

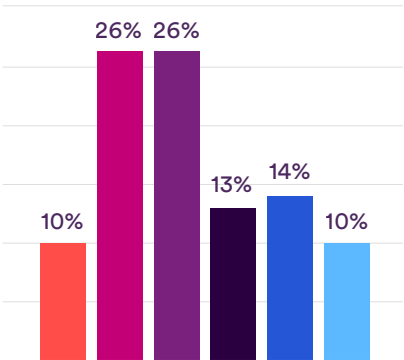
Physical security employee count

1 - 20	43%
21 - 200	34%
201 - 1,000	12%
1,001+	9%
None	2%

END USER RESPONDENTS BY THEIR ORGANIZATION'S NUMBER OF PHYSICAL SECURITY DEPARTMENT EMPLOYEES.

Video surveillance deployment (# of cameras)

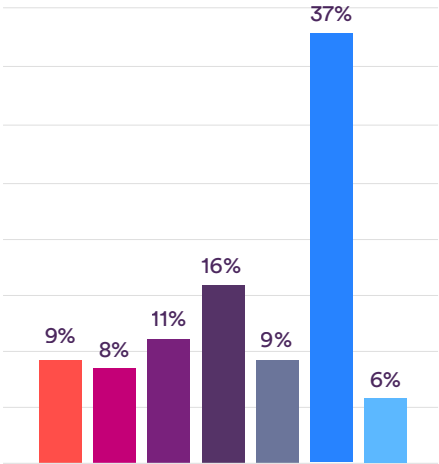
1 - 10	10%
11 - 100	26%
101 - 500	26%
501 - 1,000	13%
1,001 - 5,000	14%
5,001+	10%



END USER RESPONDENTS BY TOTAL NUMBER OF VIDEO SURVEILLANCE CAMERAS DEPLOYED.

Access control badge holders

20 cardholders	9%
21 - 50 cardholders	8%
51 - 100 cardholders	11%
101 - 500 cardholders	16%
501 - 1,000 cardholders	9%
1,001+ cardholders	37%
None of the above/not applicable	6%



END USER RESPONDENTS BY TOTAL NUMBER OF ACCESS CONTROL BADGE HOLDERS.

Appendix 4 – Respondent comments

Survey participants were able to provide additional comments associated with some survey questions. The following are selected responses that are representative of overall sentiments.

End users: What technology do you have deployed in the physical security environment at your organization?

- Alarm management/alarms
- Armed physical security/security staff
- Building management systems (BMS)
- Border management
- Canines
- Crisis management
- Custom access keys
- Drones
- Duress systems (Lynx; fixed and wireless)
- Fire detection and evacuation, armored vehicle monitoring, art protection, vault protection
- Gate security (bollards, barriers, walk-through metal detectors, x-ray screening, speed gates)
- Key management storage solutions/ key control
- Key safe cabinets
- McAfee Total Protection
- Physical key management cabinets (Traka)
- POS integration in internal theft control
- Public safety
- Robotics and drones
- Training
- Transmission of images from helicopters and drones
- Video protection

End users: What are the core functions of your physical security operations?

- Access control (biometric/RFID), personal access, and door/gate control
- Alarm management and public space surveillance (including city/public road surveillance)
- CCTV surveillance across sites, with local monitoring/recording and analytics for proactive detection
- Centralized control and monitoring by the administration/management team (on-site and from home)
- Event security and checkpoints (patrol officers, metal detectors; corporate/public festivals with law enforcement agencies)
- Identification of suspicious behavior by operators (non-AI) and after-the-fact investigations
- Monitoring and management of communications equipment and perimeter security firewalls
- Perimeter protection (fencing, motion sensors, intrusion alarms)
- Physical identity and access management/ physical security information management integrated on the same platform
- Regular site patrolling to monitor sensitive zones and respond to anomalies in real time
- Staff and service monitoring; system maintenance
- Strategy and compliance activities
- Training (staff education and readiness)

- Transmission of images by helicopter and drone to operations centers
- Use of badging data with real estate data to inform facilities decisions

End users: What are the primary reasons your organization chose a hybrid-cloud deployment?

- Analytics, LLM, federation
- Data security, information security, and compliance features
- Flexibility to use when not on a corporate network
- Necessity for some license plate recognition devices
- Preventing data loss due to physical damage
- Reduce load on server team
- Remote area service capability
- Video sharing

End users: What is your organization trying to achieve by integrating AI with your physical security systems?

- Collect vehicle video and link it with AI to analyze traffic volumes and optimize signal systems
- Detect suspicious behaviour
- “In all honesty, I would like to integrate all of the above”
- Monitor the system operation process
- Necessity for some license plate recognition devices
- Security

End users: What were the top challenges faced by your organization in 2025?

- Balancing modernization with auditability and investor transparency
- Budget constraints

- Geo-political and economic changes; geopolitical threats
- Installation of a video surveillance system (execution pressure)
- Layoffs
- Security (general operational risk)

End users: What type of project will be the focus of your department for 2026?

- Expansion of video protection
- Facial recognition; weapon detection
- Integration of key management systems into access control
- IT ticket resolution; telephony (shared infra/ IT touchpoints)
- Medicine and health data analysis and control (sector-specific)
- Monitoring store-level sales/purchase/damage data (business-ops adjacency)
- Move toward a unified system
- Replacement of analog cameras with IP systems

End user: Which of the following remote connectivity capabilities are you interested in?

- Cloud usage not allowed under company or government policy
- Concerned about cloud access speed and footage retrieval delays
- Concerned about video archive traffic on WAN links
- Concerned about lack of direct control over cloud policy (follow IT recommendations)
- Evidence management and digital case sharing
- Hybrid connectivity
- Local data storage, as mandated by regulatory and operating requirements

- On-premises cloud
- Visitor management and physical access management tools

Channel partners: What kind of physical security technology does your organization most commonly install or deploy?

- Access control systems, video surveillance, intrusion detection, and automation platforms
- Cloud-enabled and AI-based analytics deployments
- Critical communications, smart-asset management, and body-worn cameras
- Drones and smart-road video solutions for perimeter and traffic monitoring
- Electronic fencing with license plate recognition and vehicle gate automation
- Fire alarm and detection systems integrated with BMS
- GSOC, NOC, firewall, IDS, and extended detection and response solutions
- Master-key and key-management systems, including mechanical and hybrid devices
- Physical security offered as a managed service (PSaaS/GSaaS)

Channel partners: Which legacy systems are most often being replaced by your customers?

- Aging Mercury MR-52 boards
- Biometric and facial-recognition systems upgraded for accuracy and integration compatibility
- Legacy intrusion sensors replaced with intelligent, network-based detectors
- Network hardware (switches, servers, routers) modernized to support hybrid-cloud environments
- Outdated SIP phones and desktops

Channel partners: What type of projects do you expect will drive your business in 2026?

- AI-powered video analytics and automation projects integrating across HR, facilities, and compliance functions
- Cloud-based services, including GSaaS, VSaaS, and hybrid deployments
- Custom integrations within existing enterprise platforms
- Data center and server virtualization projects supporting secure infrastructure
- Ecosystem access management and digital lock deployments
- Fire detection, alarm, and BMS-integrated safety systems
- Full-scope security modernization combining multiple vendor platforms
- Integrated command-and-control solutions combining access control, video, and data intelligence
- Physical security and data center protection initiatives, including industrial and school safety retrofits
- Responsible AI development, governance, and policy-oversight frameworks

Channel partners: How has the growing trend of machine learning, artificial intelligence (AI), and/or large language model (LLM) applications impacted your business?

- AI and LLM applications driving demand for smarter analytics, predictive monitoring, and automation
- Created a dedicated AI department to integrate new capabilities into existing security products
- Customers increasingly requesting AI-enabled products and training, prompting upskilling across teams
- Expecting tighter AI integration in video surveillance to reduce operator workload and improve response efficiency

- Managing unrealistic expectations due to vendor marketing
- Many clients lacking understanding of AI's practical applications
- More customer demands for specific AI within their video solutions
- View of AI as a risk or “too manipulative”
- “We plan on providing AI-powered services to customers”

Channel partners: What do you expect could cause project delays in 2026?

- Budget delays and cost approvals
- Certification and import requirements (STQC, BIS-ER, etc.)
- Conservative end user budgets
- Coordination delays
- Customer decision-making slowed by cost controls and political uncertainty
- Economic pressures and inflation
- Ongoing supply chain disruptions for hardware
- Political and regulatory instability (elections, regional conflicts)
- Shortage of skilled professionals, especially in AI and cloud
- Training and upskilling needs

Consultants: Has anything else slowed your customers' adoption of cloud-based solutions for physical security applications?

- Control over data (security, availability) and fees
- Cost and management efficiency
- Cybersecurity and regulatory compliance issues
- Data security and control concerns
- GDPR and data-residency requirements

- IT department resistance and internal policies
- Lack of education and understanding of cloud systems
- Limited connectivity and bandwidth for video
- Vendor lock-in and recurring subscription costs

Consultants: When it comes to cybersecurity, what specific actions/approaches has your organization taken to educate customers?

- Awareness programs and staff training
- Client education on GDPR, HIPAA, and PCI DSS obligations
- Educational marketing and consulting
- ISO 9001 certification and compliance frameworks
- Organizational policies and best practice guidance
- Requiring installers to meet CISA/manufacturer standards

Consultants: What were the top challenges faced by the majority of your customers in 2025?

- Compatibility with obsolete infrastructure
- Expected budget cuts
- Legislation on private data and database interconnection
- Limited AI knowledge (big data/analytics)
- Rising licensing and maintenance costs
- Shortage of qualified integrators

Consultants: What type of projects do you think your customers want to prioritize for 2026?

- Integration of technologies and developments
- Integration with GCC and regional systems

- New technologies for high-value cargo protection
- Replacing physical security officers with technology
- Situational awareness tools to share data across business units

Consultants: Are there concerns within your clients' organizations about implementing AI technology in their physical security environment?

- Cost premium and unclear purpose
- Data privacy and compliancy concerns
- Fear of replacing human expertise
- Reliability and trustworthiness of AI output
- Waiting for AI to mature before adoption

Consultants: What type of projects do you think your customers want to prioritize for 2025?

- Card encryption and card changeouts
- Something in the area of sustainability

Consultants: What are customers asking about in terms of how to best manage access control data?

- Cybersecurity and data-backup practices
- Guidance on secure storage and recovery procedures
- Most customers follow installer or vendor recommendations



About Genetec

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

Based on an open architecture and built with cybersecurity at their core, Genetec products are world-leading in video management, access control, and ALPR. Other solutions offered by the company include products for intrusion detection, intercom, and digital evidence management.

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

To learn more about us, visit
[genetec.com](https://www.genetec.com)

For more information about this report,
please contact Genetec-research@genetec.com

Genetec Inc.
[genetec.com/locations](https://www.genetec.com/locations)
info@genetec.com
[@genetec](https://www.genetec.com)

© Genetec Inc., 2025-2026. Genetec and the Genetec Logo are trademarks of Genetec Inc., and may be registered or pending registration in several jurisdictions. Other trademarks used in this document may be trademarks of the manufacturers or vendors of the respective products.