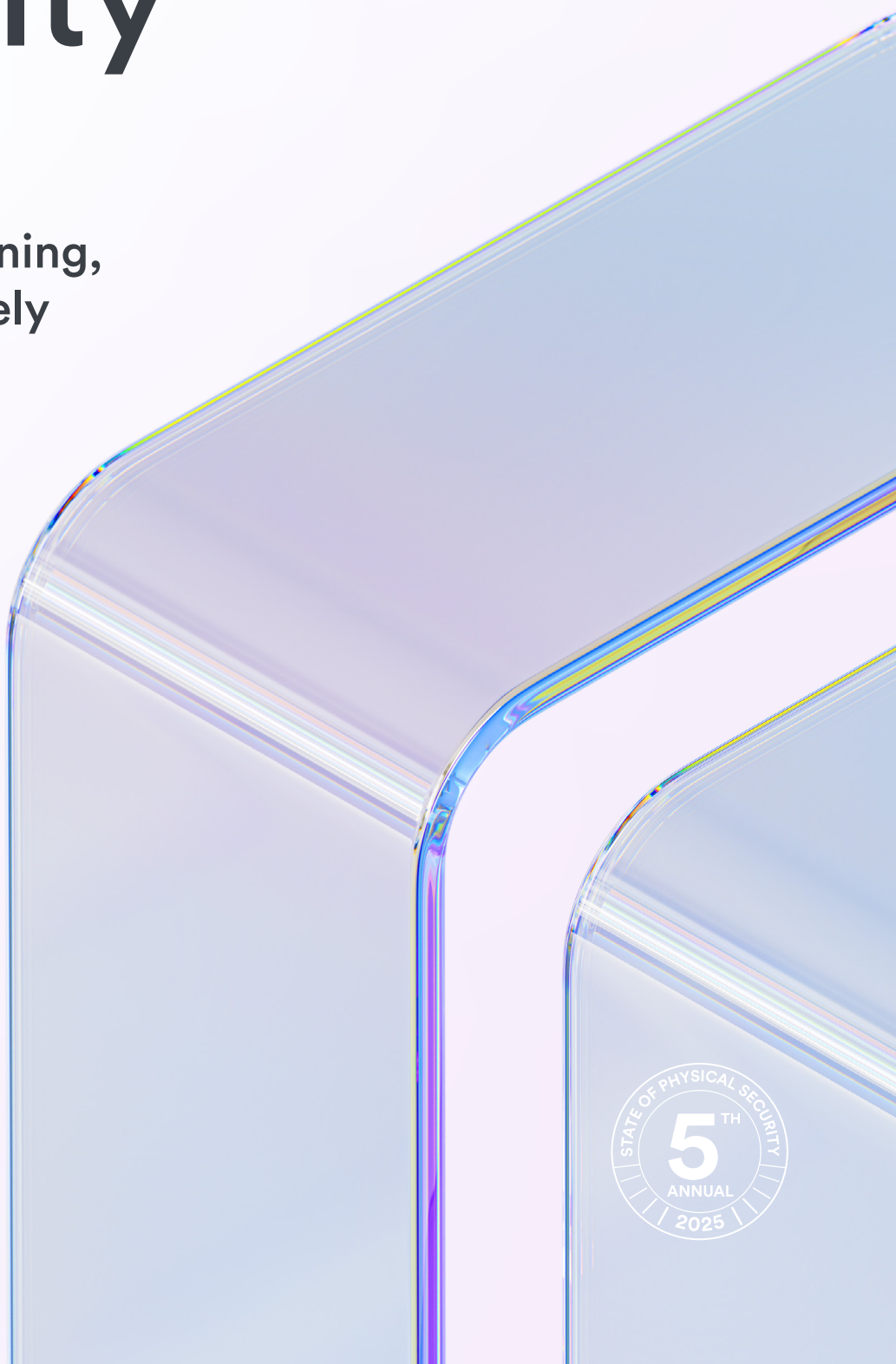
State of Physical Security 2025

Strategizing, planning, and investing wisely



Genetec™

Contents

About the research

Genetec Inc. surveyed physical security professionals from around the world between August 12 to September 15, 2024. Following a review of submissions and data cleansing, 5,696 respondents were included in the sample for analysis.

The goal of the research was to:

- Gain insights into physical security operations and environments in 2024
- Identify the outlook for physical security projects for 2025
- Understand upcoming challenges

Summary of survey methodology

The target population for the survey focused on three main groups:

End users

Individuals working for organizations participating in the procurement, management, or use of physical security technology.

Channel partners

Individuals who consult, install, service, or produce physical security solutions.

Consultants

Individuals who consult on the design, installation, maintenance, and operation of physical security solutions.

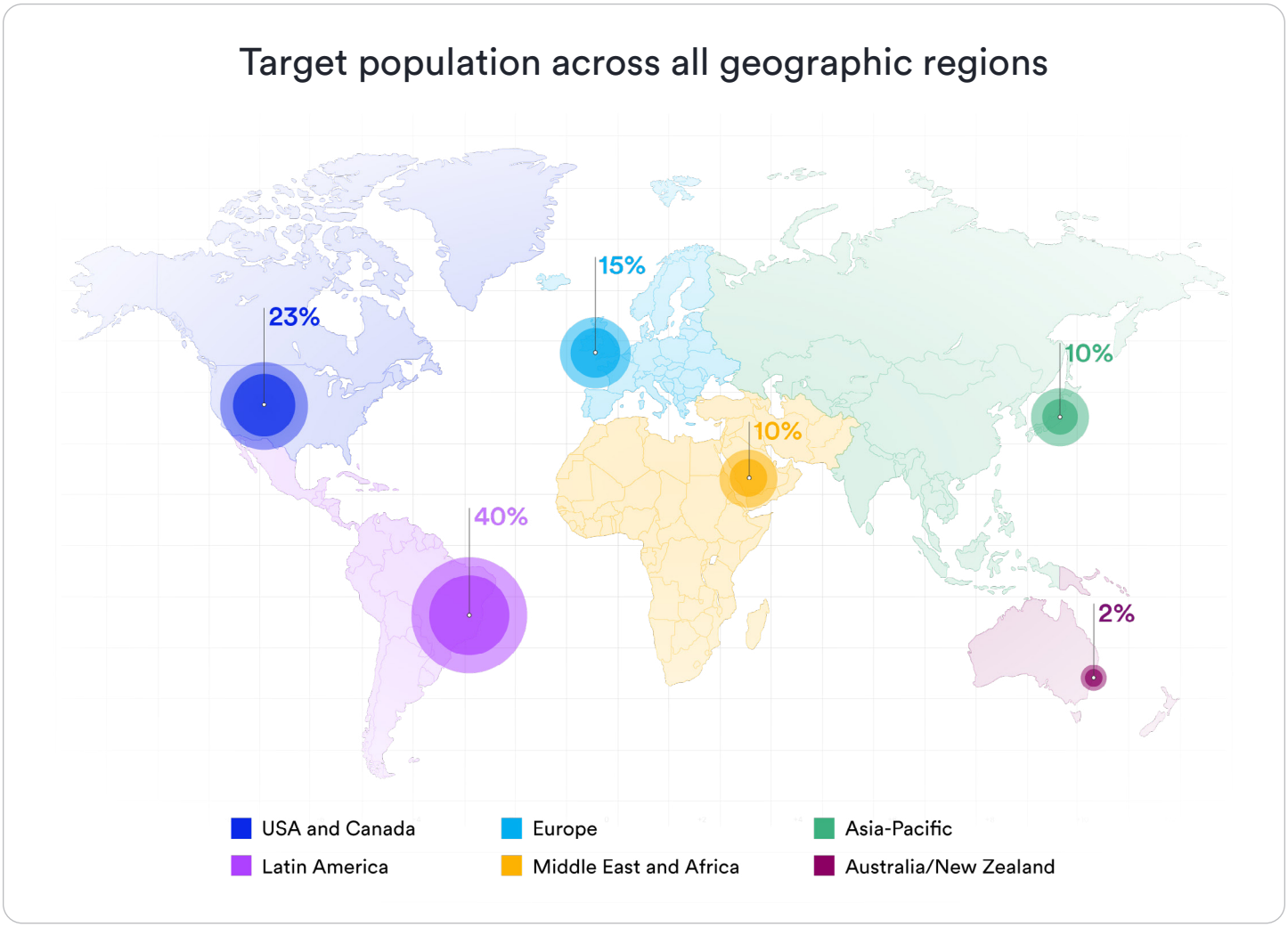


FIGURE A: PROPORTION OF RESPONDENTS BY REGION.

- The target population was reached through in-person events, and by third parties through their opt-in email lists, Genetec opt-in email lists, and by digital promotions.
- One set of survey questions was asked to end users and a different set of questions was asked of channel partners and consultants.
- This report points out whether answers are from end users, channel partners, consultants, or all respondents.
- Only fully completed surveys submitted by individuals within the targeted population were included in the final analysis.
- In most of the survey, there was little significant difference between the responses received from the different geographic regions. For more details about these differences see the “Summary of differences from around the world.”

For more details about the survey methodology and demographics of the respondents please see Appendix 1 and 2.

Executive summary

This year's report documents interesting changes in the physical security industry. Based on the data collected, we see some surprising shifts in priorities and a renewed focus on operational excellence. In 2024:

57% of end users say the top challenges were aging outdated physical security and/or information technology (IT) infrastructure

65% of channel partners say their clients want to benefit from new tech and capabilities

66% of end users ranked access control (50%) and/or video surveillance (39%) as top processes or capabilities for the year. This aligned with 81% of channel partners' work focusing on either of these core systems

49% of end users in 2024 reported 100% on-premises deployments of physical security (no cloud)

77% of end users say physical security and information technology (IT) departments work collaboratively

Global key findings

Economy impacts project timelines

49% of end users delayed projects in 2024 and 45% in 2023. But the reasons were very different. In 2023 supply chain issues were the main reason, but in 2024 the cause was economic uncertainties.

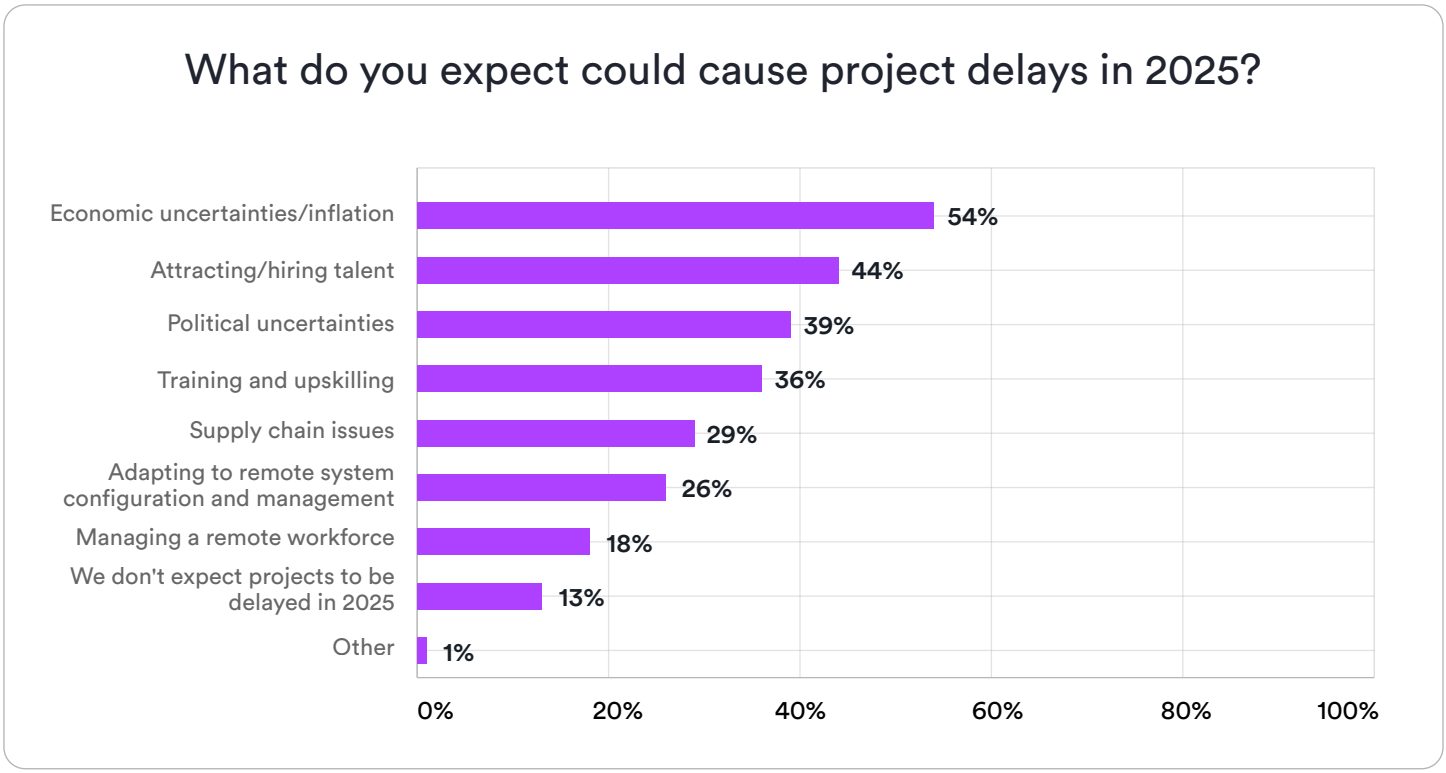


FIGURE B: TOP EXPECTED CAUSES FOR PROJECT DELAYS IN 2025.

Insights

Political changes could also have played a role. Time magazine referred to 2024 as being “the election year” with at least 64 countries including the USA, India, Taiwan, South Korea, and the UK holding key national elections in 2024.[1]

[1] Elections Around the World in 2024 | TIME

Recruiting challenges persist

Since 2021, both end users and channel partners have consistently reported staffing issues. And the outlook for 2025 points to ongoing concerns. 72% of channel partners expect to continue to have hiring challenges while only 6% believe it will improve.

Channel partners also expect these talent shortages to impact their projects, with 44% saying that attracting and hiring workers will cause project delays in 2025.

76%

of channel partners said that "Installation Technician" is the toughest role to fill

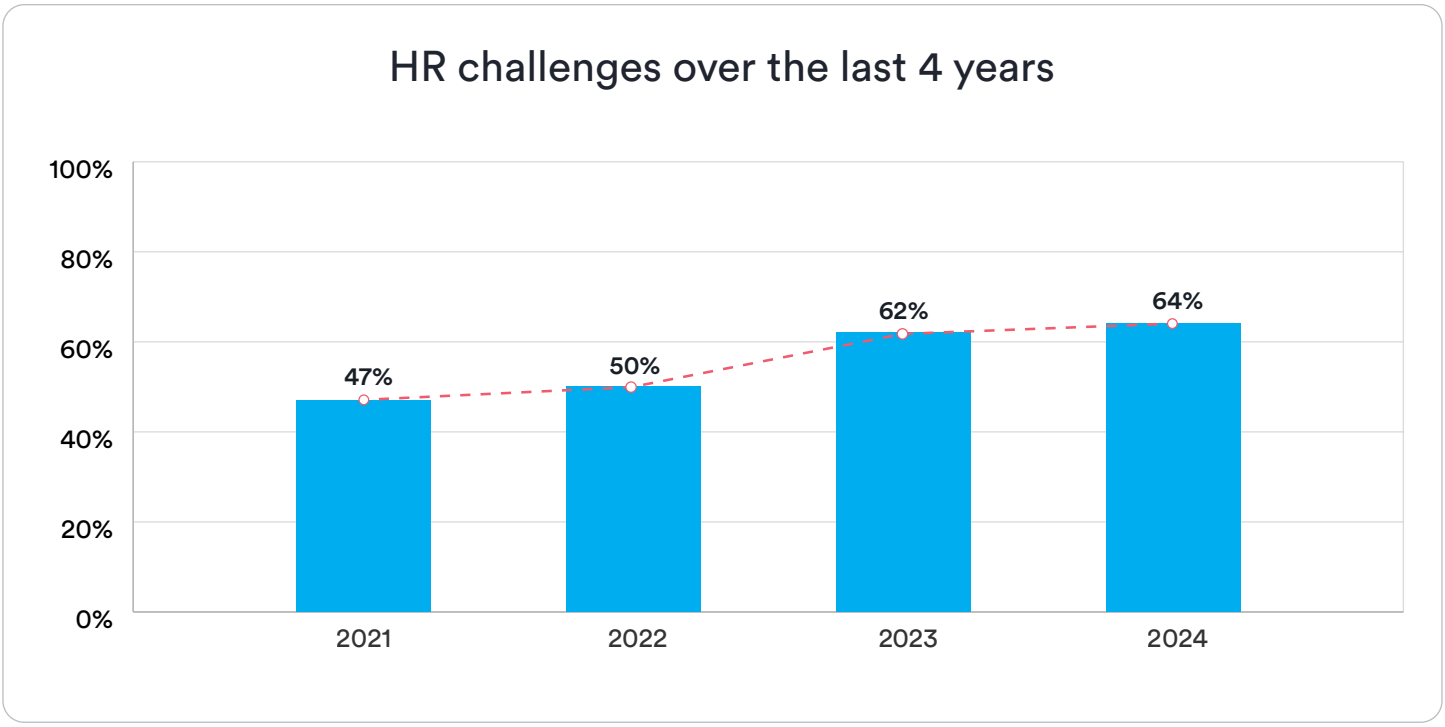


FIGURE C: PERCENTAGE OF CHANNEL PARTNERS THAT EXPERIENCED HR CHALLENGES (2021-2024).

“To succeed, end users in the physical security space require the support, training, and services that help them get the most value from their investments in technology. Partnering with recognized security experts through the deployment and lifecycle of their selected solution ensures they can maximize their investment and build an effective, reliable and scalable physical security posture for their organization.”

Nadia Boujenoui
Vice-President of Customer Experience and Operations
Genetec Inc.

Budgets adjust

Operational expenditure (OpEx) budgets in 2024 didn't align with 2023 predictions, where over 50% of respondents expected steady or increased OpEx budgets. Instead, 44% reported an increase or steady OpEx budget. Capital expenditure (CapEx) budgets also held stable, with only 17% of end users noting a decrease. Amid economic and political uncertainties, these slight adjustments highlight the physical security industry's pragmatism and the essential role these systems play in organizations worldwide.

48%

of respondents stated that their CapEx budget increased or remained flat in 2024. Of this group 48% indicated that it increased between 11-25%

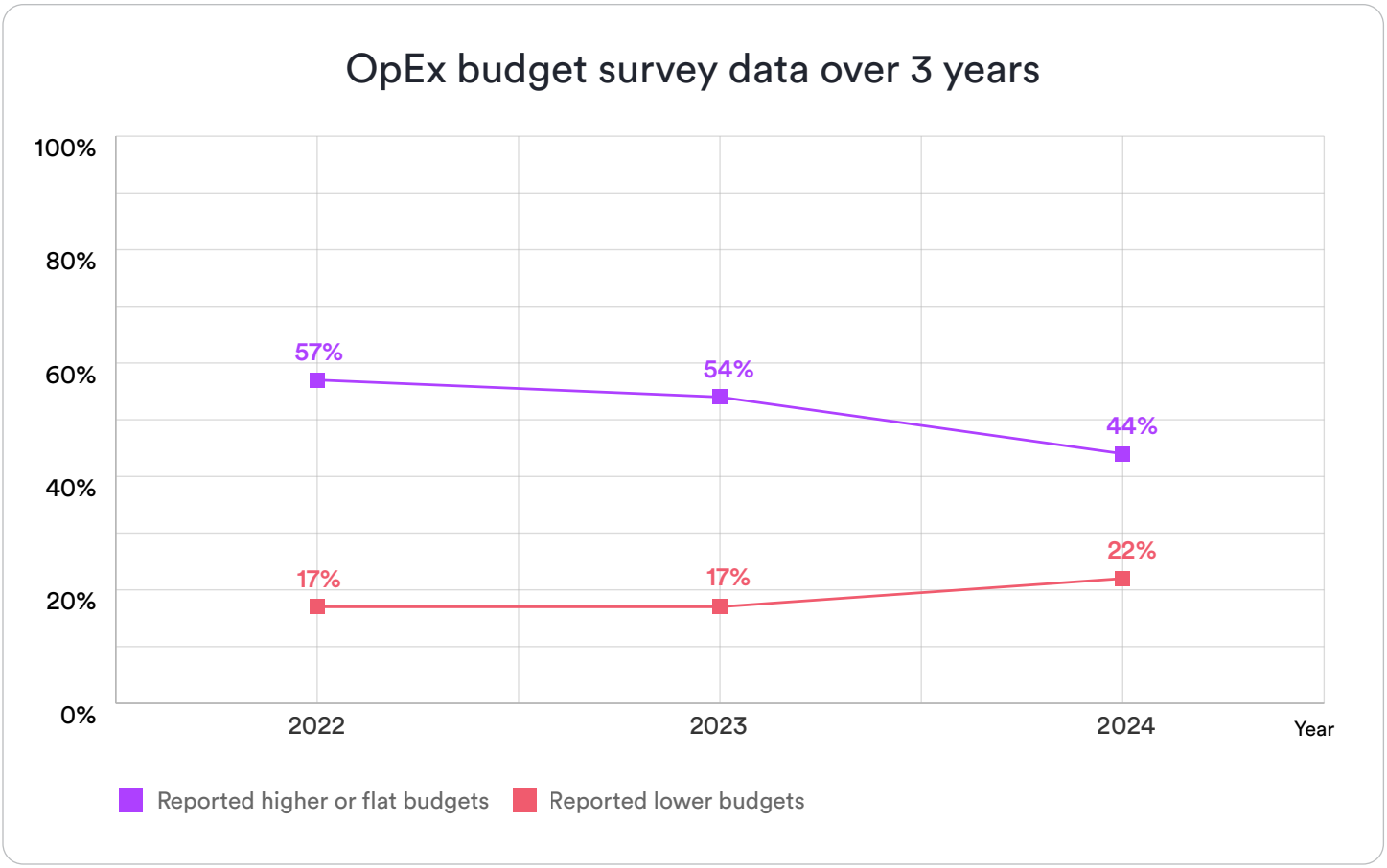


FIGURE D: PROPORTION OF RESPONDENTS REPORTING OPERATIONAL EXPENDITURE BUDGETS INCREASED, REMAINED FLAT, OR DECREASED (2022-2024).

Cyber resilience remains a priority

As cyber threats continue to rise, more end users are taking action to strengthen their cybersecurity. Organizations are using guidance from industry regulations and cybersecurity partners that have the expertise to create plans and put them into motion.

38%

of consultants indicated that they're planning to grow their coverage into cybersecurity

Top cybersecurity practices implemented

	2023	2024
Educating users on cybersecurity best practices	61%	71%
Fine-tuning user permissions and privileges	42%	51%
Securing data storage	41%	47%
Hardening security infrastructure	47%	44%
Protecting the system from unauthorized access	42%	44%

FIGURE E: PROPORTION OF RESPONDENTS THAT IMPLEMENTED CYBERSECURITY PRACTICES (2023-2024).

Industry regulations are also propelling improvements in data protection and cyber resilience. In 2024, 67% of end users said their organization was affected by these regulations, a big jump from just 13% in 2023. Examples like NIS2 compliance, GDPR, and other industry-specific rules were repeatedly mentioned.

"As society is waking up to the kinds of disruption that immature cybersecurity can have on daily lives, governments around the world are implementing more directives and regulations. Unsurprisingly, this has made its way to the physical security industry, with the effect of increasing our attention to our overall security posture."

Mathieu Chevalier
Manager and Principal Security Architect
Genetec Inc.

“A company that does not comply with privacy and data protection laws, and that does not adopt the necessary measures to safeguard the personal data it handles and stores, is a company that will end up losing the trust of its customers, its employees, its partners and its shareholders. In the long run, it will result in economic losses.”

–Consultant respondent

Cloud adoption meets physical security realities

Cloud adoption in the physical security industry grew fast between 2022 and 2023 while results in the most recent 2024 survey revealed a deceleration. In 2024, 38% of end users reported that over 25% of their physical security environment was cloud or hybrid cloud – down 6% from 2023.

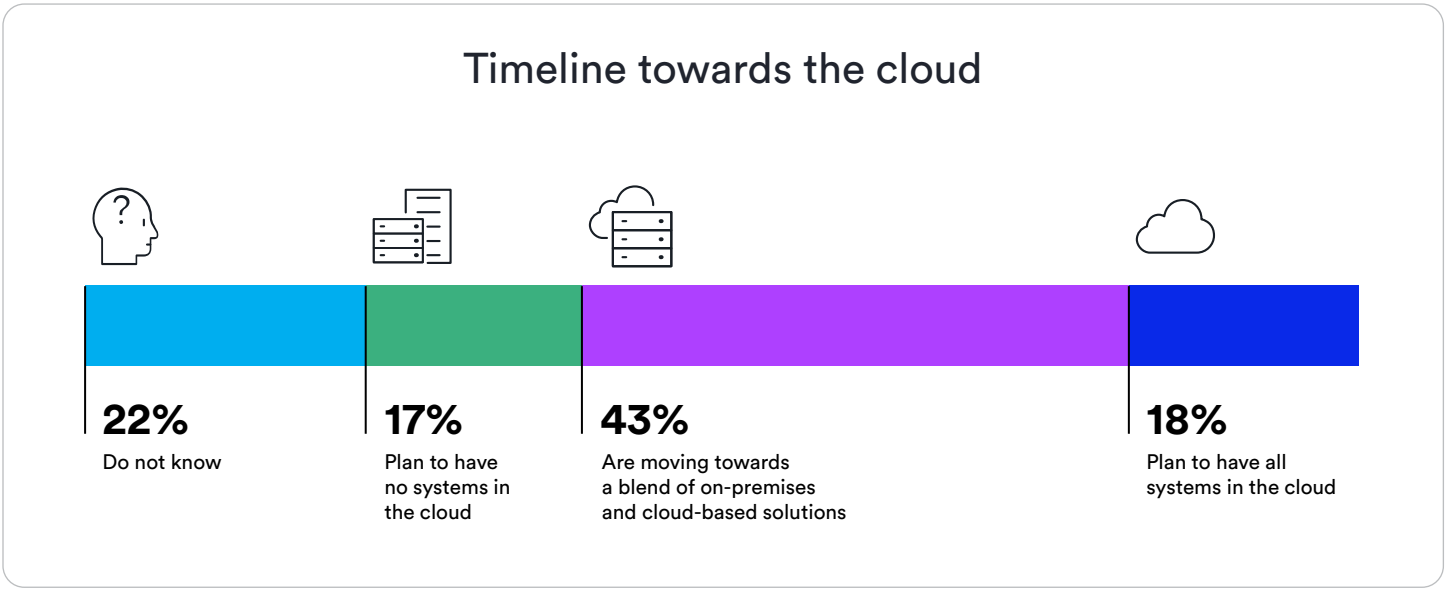


FIGURE G: PROPORTIONS OF RESPONDENTS PLANNING TO INCORPORATE CLOUD.

When end users were asked what has impacted their organization's adoption of cloud solutions, budgetary reasons related to "cloud storage, data retention, and bandwidth costs" were reported. "Fear of data loss and overall control" was their second reason, further demonstrating that physical security practitioners are looking to move workloads to the cloud in an incremental fashion, at a pace suitable for their business.

Balancing cloud adoption and cloud costs

Organizations with smaller physical security systems are more likely to use the cloud for storage, while those with larger systems are not adopting as fast. In fact, 41% of all respondents say they've slowed their cloud adoption due to costs for storage, data retention, and bandwidth.

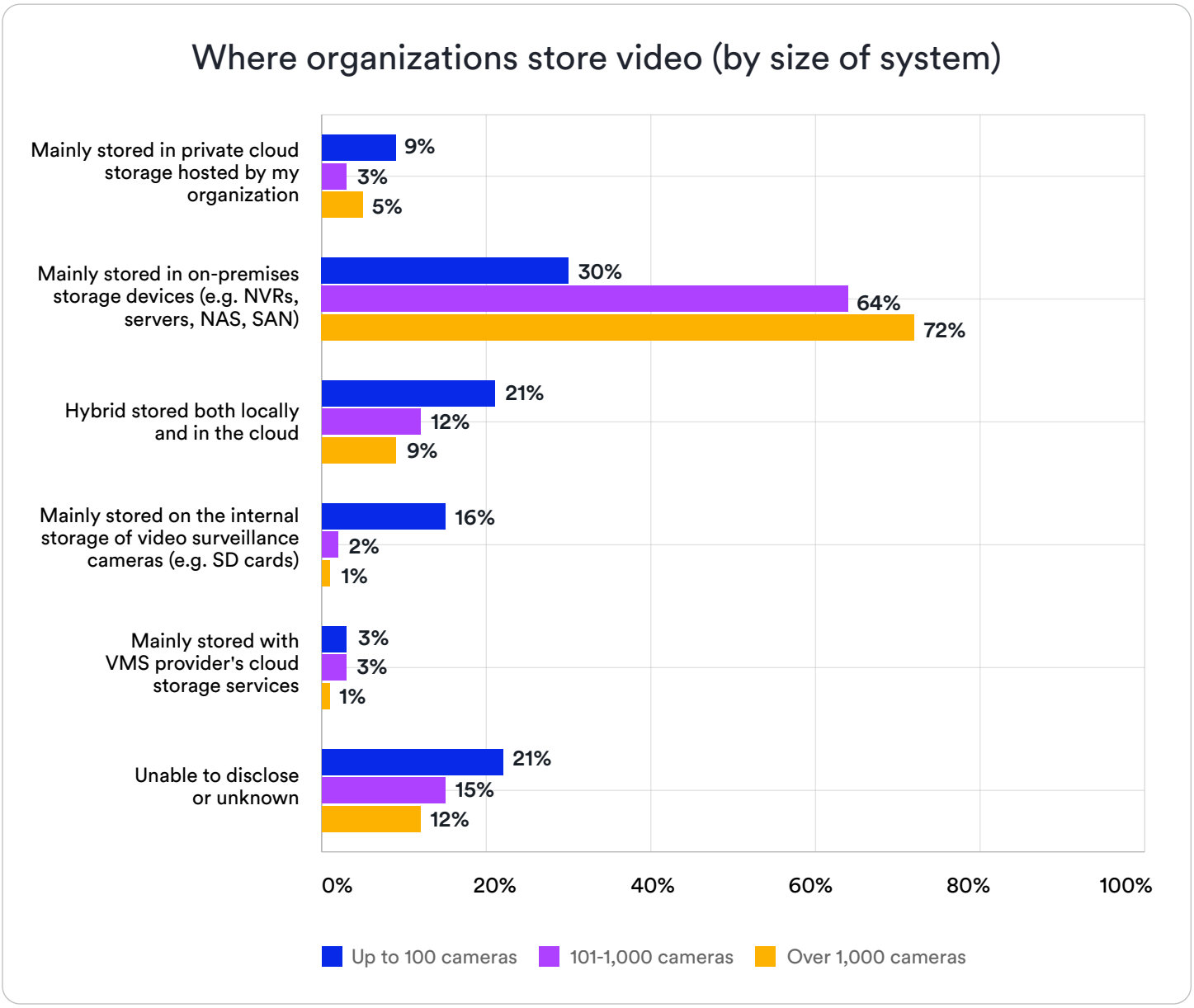


FIGURE H: DISTRIBUTION OF CAMERAS STORED LOCALLY, ON-PREMISES, OR IN THE CLOUD.

Indicators point to smaller organizations with less storage and bandwidth concerns benefiting more quickly from the convenience and accessibility of video surveillance as a service (VSaaS). In the face of deploying larger, more complex systems to the cloud, it's not surprising organizations are reviewing their investments in advance of starting work, or as the data comes in from early deployments. The need to find an optimal ROI in the cloud has become a pressing issue.

It is clear that managing cloud expenses is an emerging challenge in physical security and the issue of cloud waste is one that organizations are beginning to look at closely.

Insights

Most organizations lack proactive cloud cost-saving strategies

A Gartner survey shows that companies waste an average of 35% of their cloud spending, with waste levels ranging from 15% in well-optimized environments to 55% in unoptimized ones.

Cloud outlook is bright for hybrid deployments

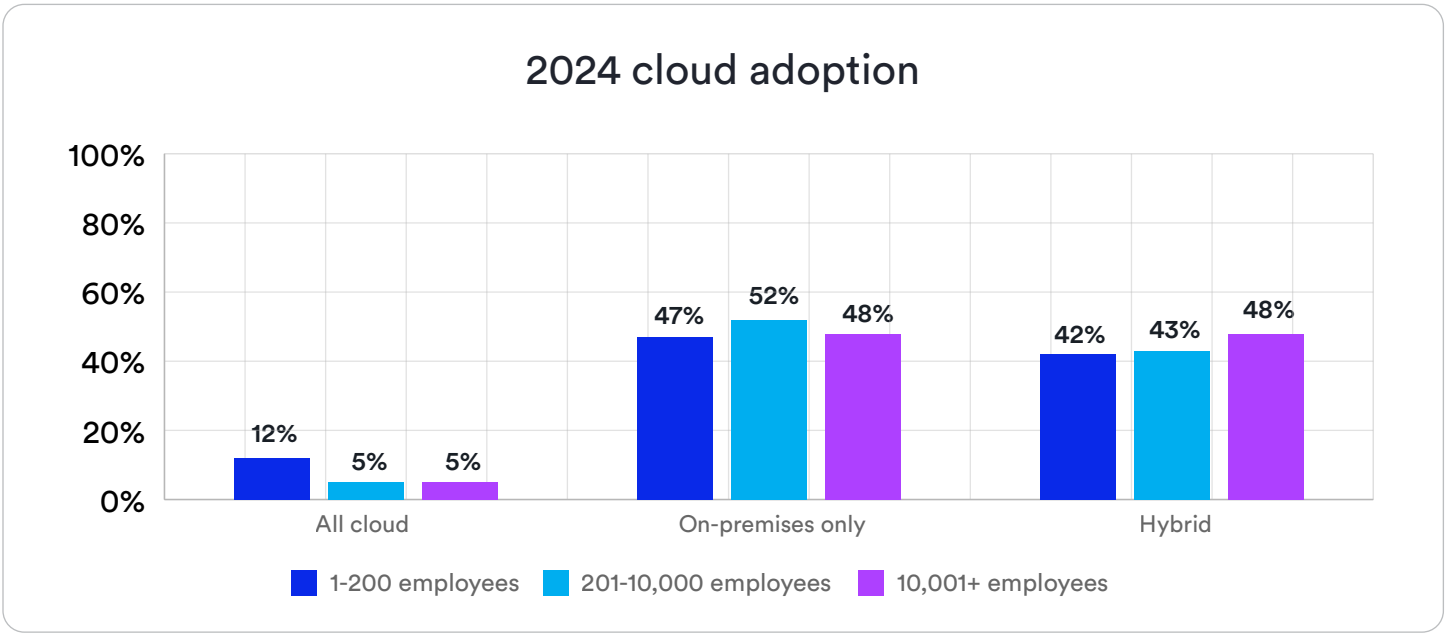


FIGURE I: CLOUD ADOPTION FOR PHYSICAL SECURITY DEPLOYMENTS.

Looking at the future of cloud adoption, it's clear from the 2024 survey results that the majority of organizations see the best way to leverage cloud successfully is through hybrid deployments. Smaller organizations, with presumably less hardware, retention, and data concerns, are predictably more interested and open to full cloud deployments.

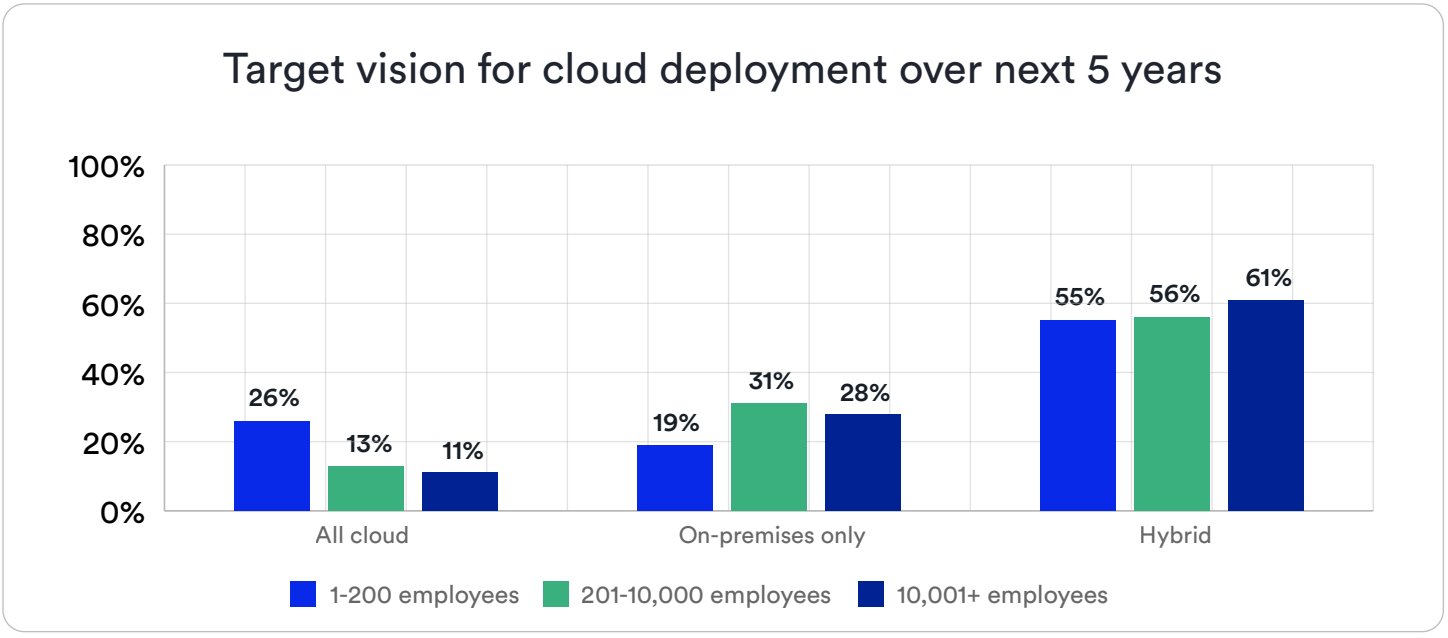


FIGURE J: FORECAST OF CLOUD DEPLOYMENT TYPE BY ORGANIZATION SIZE.

Channel partners

Channel partners are also positive about the value of cloud-based physical security systems:

78%

felt there would be an increase in new cloud systems in 2025, up from 73% last year

2%

expect a decrease, down from 5% last year

Consultants

Physical security consultants also predict cloud deployments will continue to grow:

58%

estimate that the typical timeline for their customers to move some workloads to the cloud would be within the next 12 months

66%

say they would specify hybrid-cloud security deployments over the next 5 years

25%

expect to specify full cloud deployments

Improvements of core systems continue

In 2024, 58% of channel partners saw an increase in end users "adding new technologies to existing systems, including cloud solutions". But looking ahead to 2025, 51% of end users responded that they're going to focus on leveraging existing technology like cybersecurity tools, data analysis, and improving departmental collaboration. This demonstrates that end users are looking to extract value from their existing systems and investments in new technology.

When asked to prioritize projects for 2025, all respondents put access control and video surveillance at the top of the list.

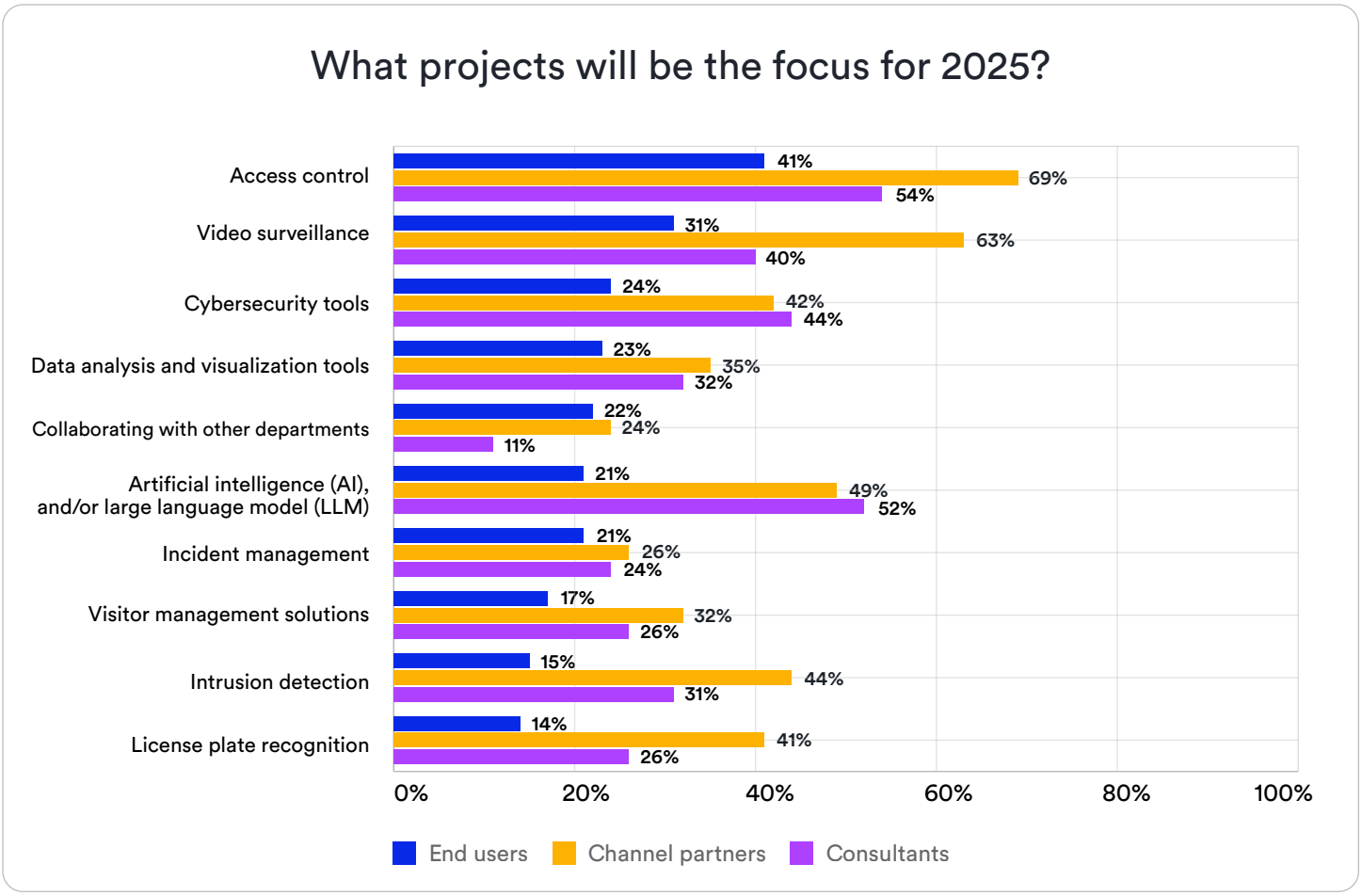


FIGURE J: TOP PROJECTS CONSULTANTS, CHANNEL PARTNERS, AND END USERS ARE PRIORITIZING IN 2025.

Insights

55% of consultants indicated their customers plan to leverage current technology to address new challenges and evaluate new systems for specific use cases.

"Year after year, respondents continue to prioritize investment in video management and access control systems, as these are central to their success. They need purpose-built solutions that deliver long-term value with the reliability, cybersecurity, and openness they can depend on. As they plan for the future, end users are looking for systems designed to grow with them, supporting their goals today and tomorrow. This includes flexible hybrid-cloud solutions that balance the benefits of cloud scalability with the control of on-premises infrastructure, ensuring optimal ROI and adaptability as their needs evolve."

Christian Morin
Vice-President of Product Engineering
Genetec Inc.

Access control investments

When it comes to access control, end users want to do more with their technology. Traditionally focused on restricting unauthorized access, end users are looking to build additional functionalities that create efficiencies and deliver a more modern approach to access. Visitor management (41%), biometrics (39%), and identity management (37%) top the list for new access control investments in 2025.

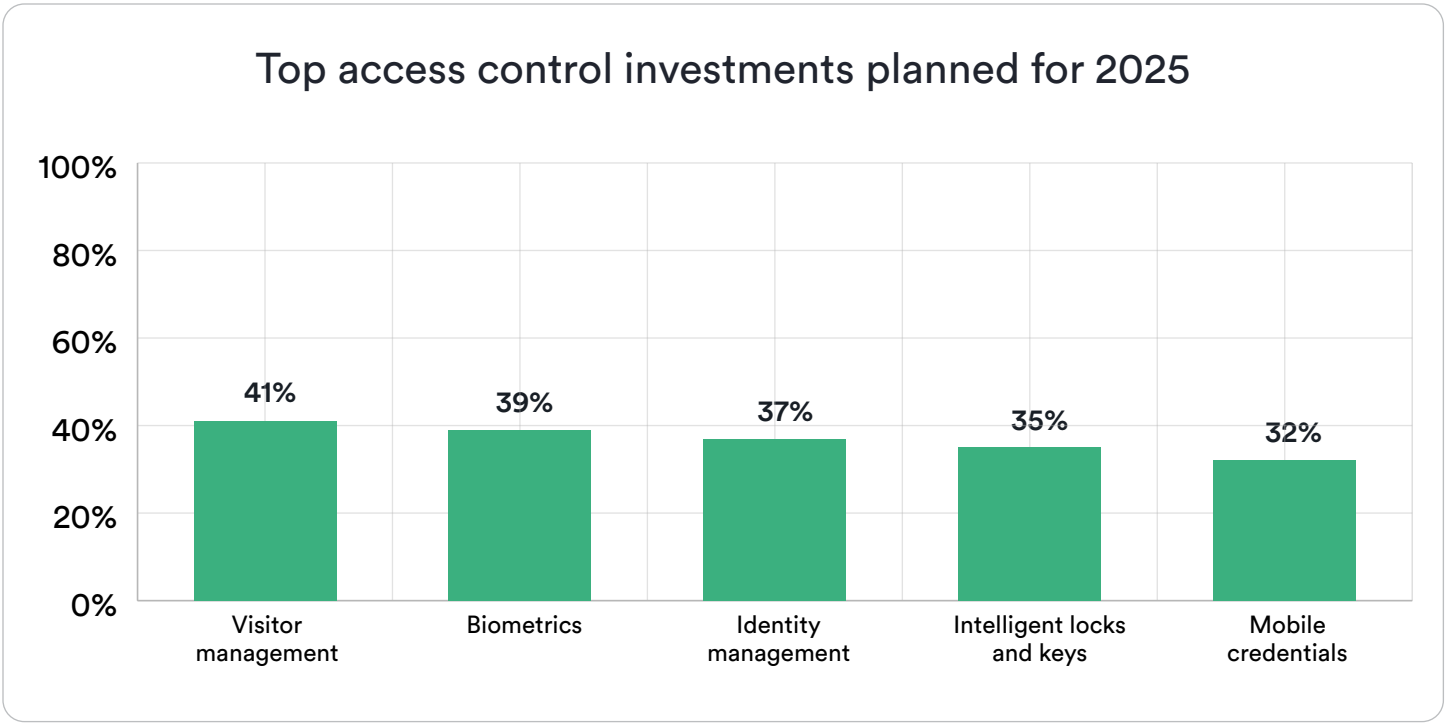


FIGURE K: DISTRIBUTION OF INTEREST IN VARIOUS ACCESS CONTROL TECHNOLOGY FOR 2025.

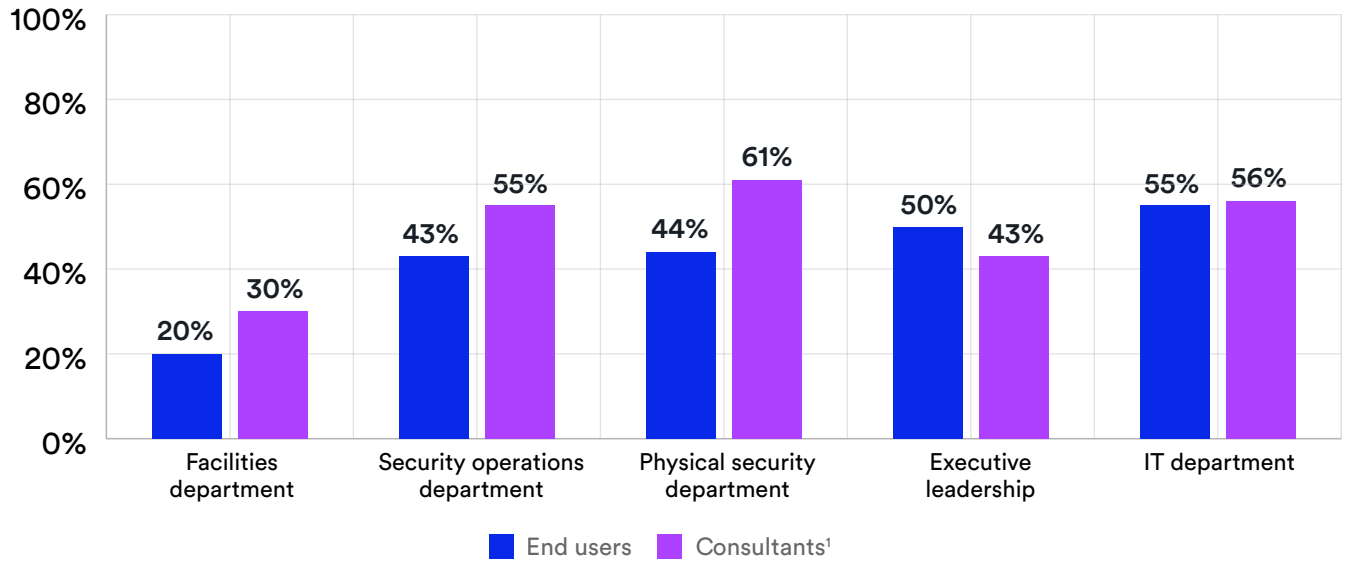
Video surveillance updates

On the video surveillance front, channel partners said end users are focused on cameras and video management systems (VMS) as key areas within legacy physical security systems to replace or update in 2025. They also reported their customers want to replace legacy systems in order to integrate new technology and get access to new capabilities, such as:

- Higher quality video
- Streamlined VMS interface
- Intelligent features in video analytics powered by deep learning

End users make the most of security data

The trend related to gathering, using, and sharing security data to improve physical security and/or business operations continued in this year's survey responses. Both end users and consultants agreed on the growing interest and use of this information across key departments.



[1] Consultants were providing their view of their customers' physical security data. Respondents could select multiple options.

FIGURE L: DISTRIBUTION OF END USER AND CONSULTANT DEPARTMENTS THAT HAVE ACCESS TO SECURITY DATA.

Physical security data is essential for shaping strategy and aligning security with business goals. Survey responses reveal that executive leaders view this data as crucial to achieving broader business objectives. Leveraging the data available in their systems allows physical security departments to play a critical role in empowering their organization's overall success as well as its safety and security.

Strategic use of security data is growing with end users wanting to improve cross-departmental work and availability of data:

23%
Want data analysis and visualization tools

22%
Want collaboration with other departments for other business outcomes

22%
Want security data democratization across the organization and better reporting

In their Security Operations Centers (SOCs), end users are also looking beyond traditional data and tasks, continuing to integrate other data to better observe, measure, and react to incidents, events, and operational requirements.

Most common data collected from other systems to use in SOCs

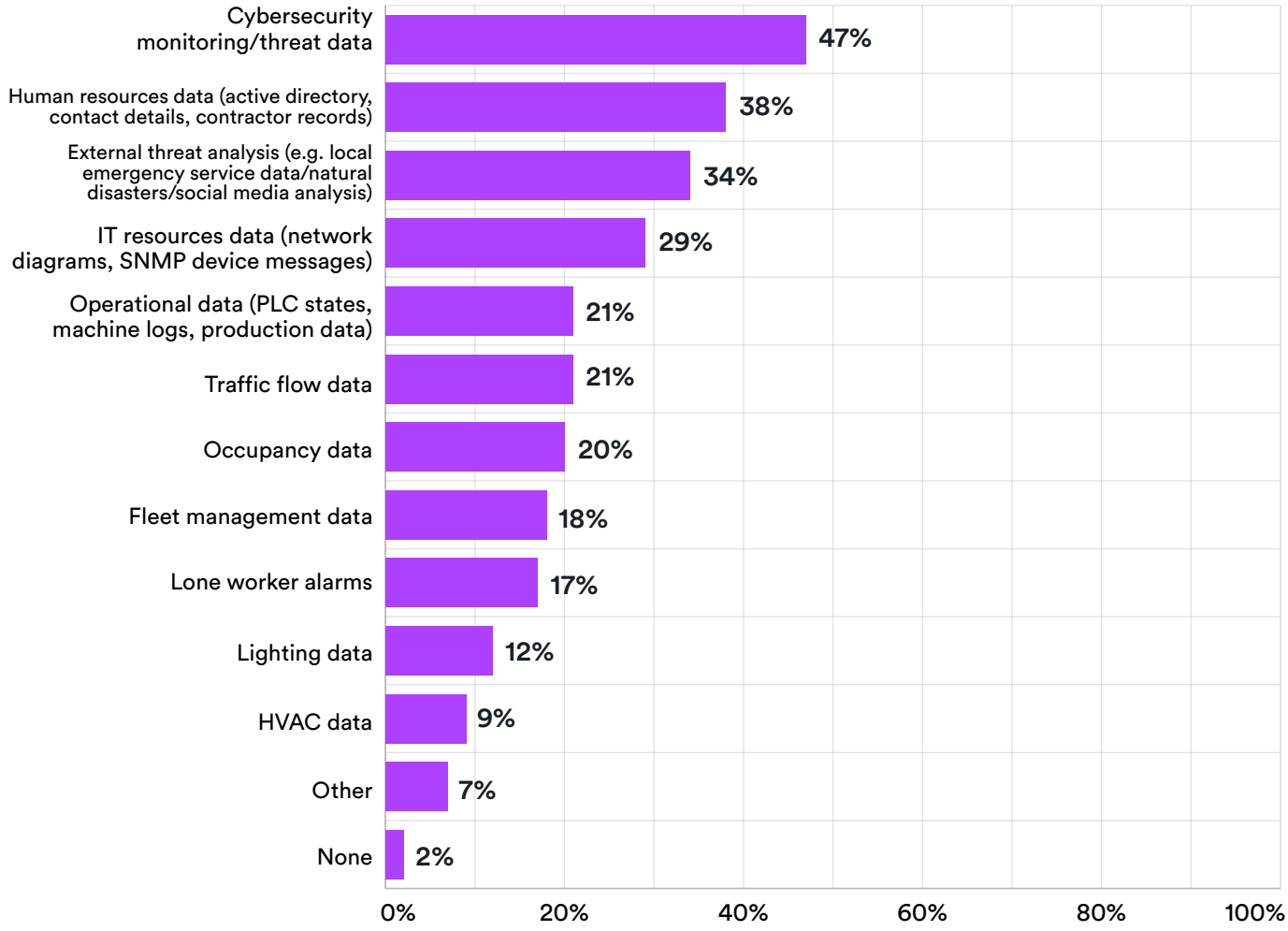


FIGURE M: DISTRIBUTION OF DIFFERENT TYPES OF DATA MANAGED IN A SECURITY OPERATIONS CENTER IN 2024.

“Physical security is the unwitting custodian of incredibly valuable data about the flows of people, assets, and vehicles. This information can guide critical decisions, but the challenge has historically been to quickly transform incidents into insights. The real opportunity for physical security is to provide visibility into these insights at a senior level and support leadership in taking action based on them.”

Pervez Siddiqui
Vice-President of Offerings and Transformation
Genetec Inc.

Understanding the value of AI

The integration of artificial intelligence (AI) into physical security systems is a promising development and one end users are eager to explore (10% did in 2024 and 37% plan to in 2025).

But figuring out where it delivers real improvements is a challenge with 27% of end users responding that they are unsure how to deploy AI in a way that adds value. 40+% of channel partners say end users want training to better understand the technology.

Of those end users that have actively engaged with the technology, most believe the value of AI will result from helping them streamline and automate different aspects of their security operations.

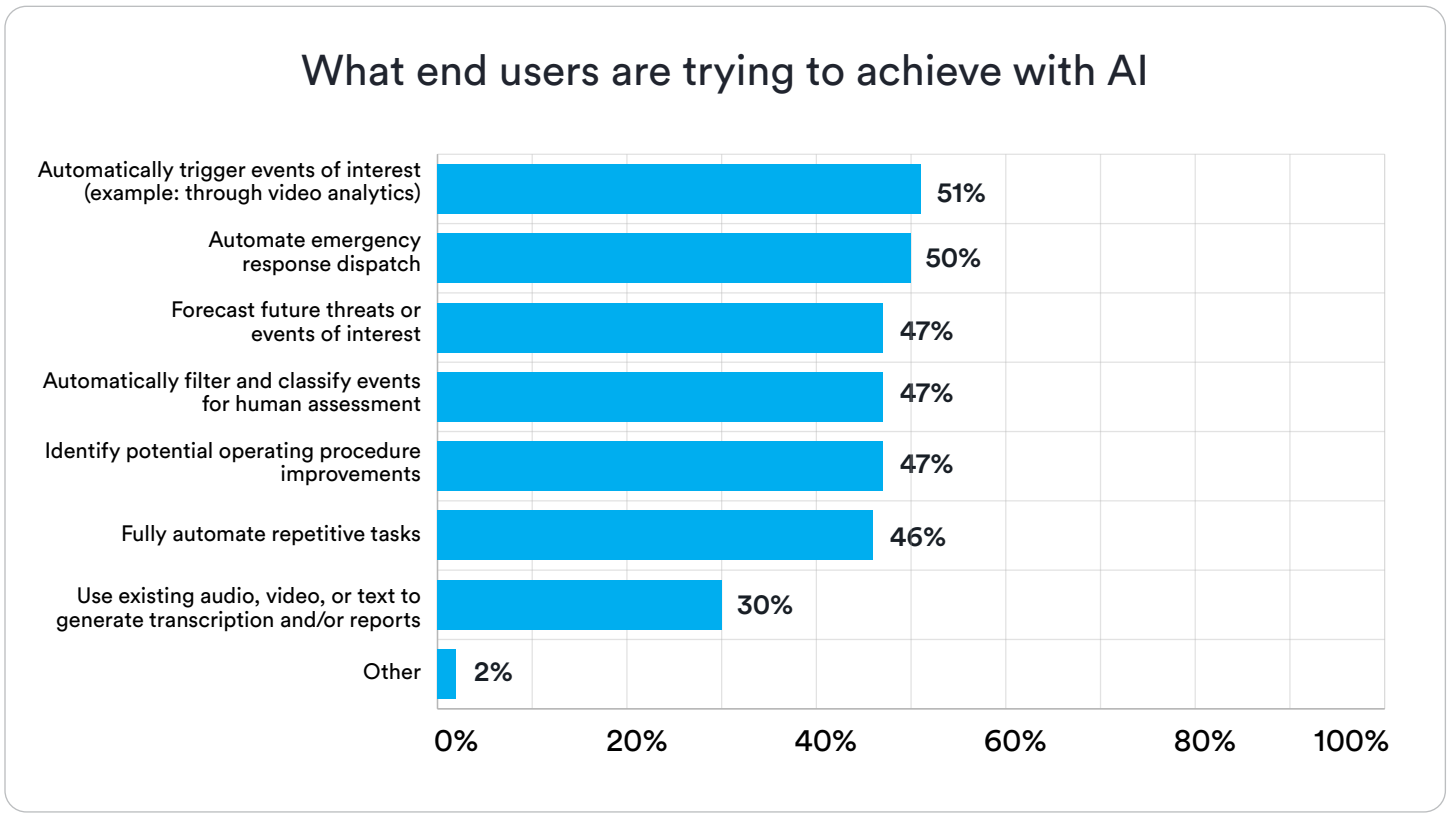


FIGURE N: DISTRIBUTION OF GOALS FOR USING ARTIFICIAL INTELLIGENCE APPLICATIONS IN 2024.

“Analytics and AI techniques will continue to usher in new possibilities, allowing businesses to capitalize on existing physical security data, infrastructure, and sensors to automate mundane tasks and drive higher levels of operational efficiency company-wide.”

Florian Matusek, PhD, MSc
Director of AI Strategy
Genetec Inc.

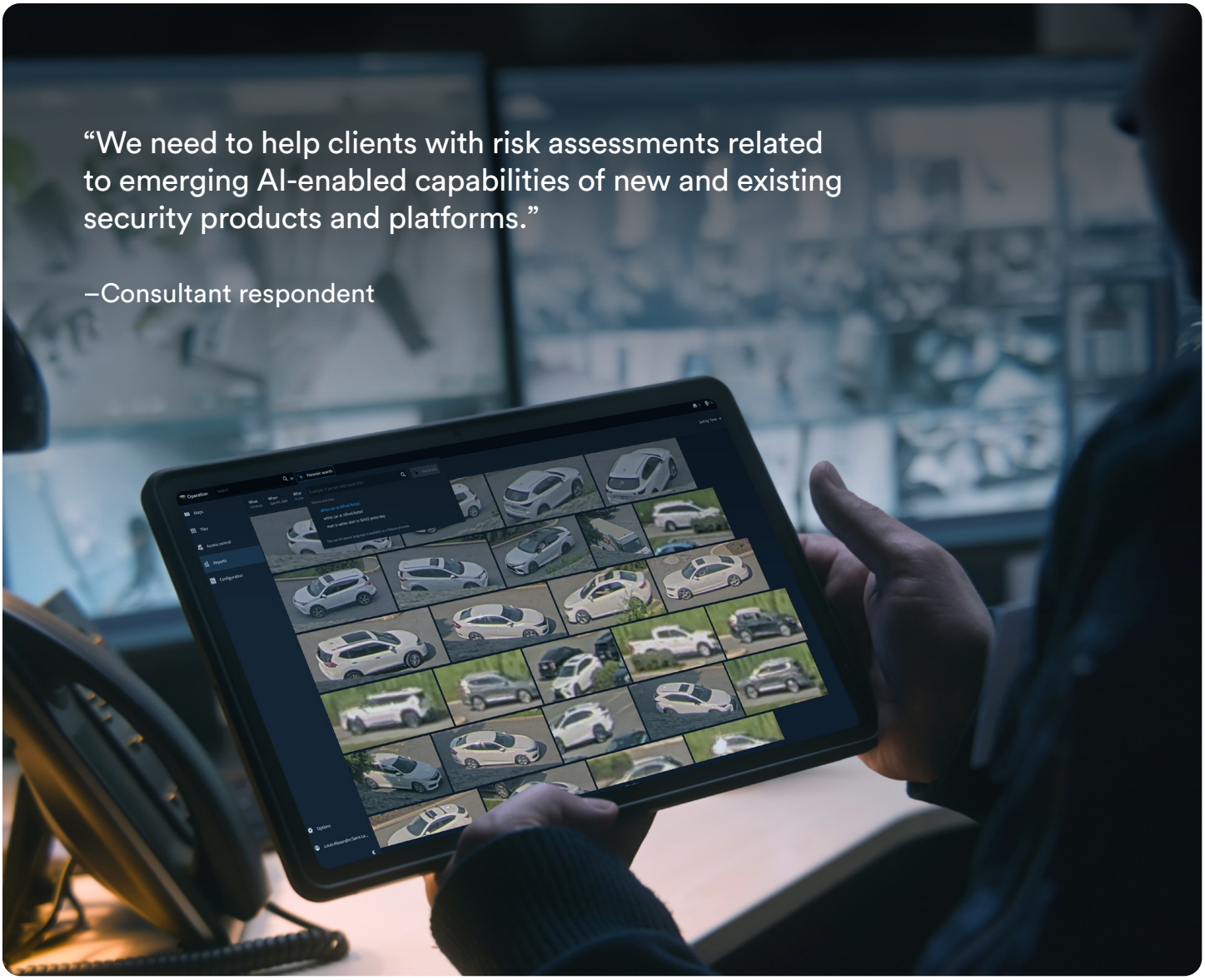
At the same time, 75% of end users expressed concerns about how AI is designed and implemented. These challenges are important for manufacturers and channel partners to address to help stimulate AI adoption and utilization in the years to come.

75%

of end users have concerns about AI design and implementation, particularly around responsible and ethical guidelines

48%

of channel partners said that end users are concerned about vendors that don't follow Responsible AI guidelines



“AI will remain dependent on human oversight and judgment for decades to come. You have the human supply the creativity and the intuition, and you have the machine do the heavy lifting.”

Pierre Racz
CEO
Genetec Inc.

IT involved in physical security decisions

Information technology (IT) continues to play a bigger role in managing and deciding on physical security systems. When respondents were asked which departments were most involved in buying decisions, IT departments consistently ranked above physical security departments.

With many departments involved in the physical security buying process, respondents also highlighted the importance of executive leadership in these often mission crucial buying decisions – most notably raised by end users.

Top 3 departments involved in 2024 purchasing decisions[1]

	End users	Channel partners	Consultants
IT department	51%	51%	51%
Physical security department	44%	44%	47%
Executive leadership	55%	36%	41%

[1] Table depicts a sub-set of departments

FIGURE O: DISTRIBUTION OF TOP DEPARTMENTS INVOLVED IN PURCHASING DECISIONS BY RESPONDENT TYPE.

"As the demands on physical security evolve, it is important to be able to support both IT and physical security teams in their adoption of existing products and the delivery of new technology. With cybersecurity, and safety and security issues at play, selecting vendors that understand and meet the capability and compliance needs of both groups becomes paramount for success."

Michel Chalouhi
Vice-President of Global Sales
Genetec Inc.

Unsurprisingly, respondents to the survey working in IT and physical security departments had different priorities related to technology deployment. In 2024, 47% of IT professionals focused on deploying cybersecurity tools, compared to 27% of security and safety professionals. Similarly, 37% of IT respondents flagged cloud-based solutions as a priority, compared to 27% from physical security respondents.

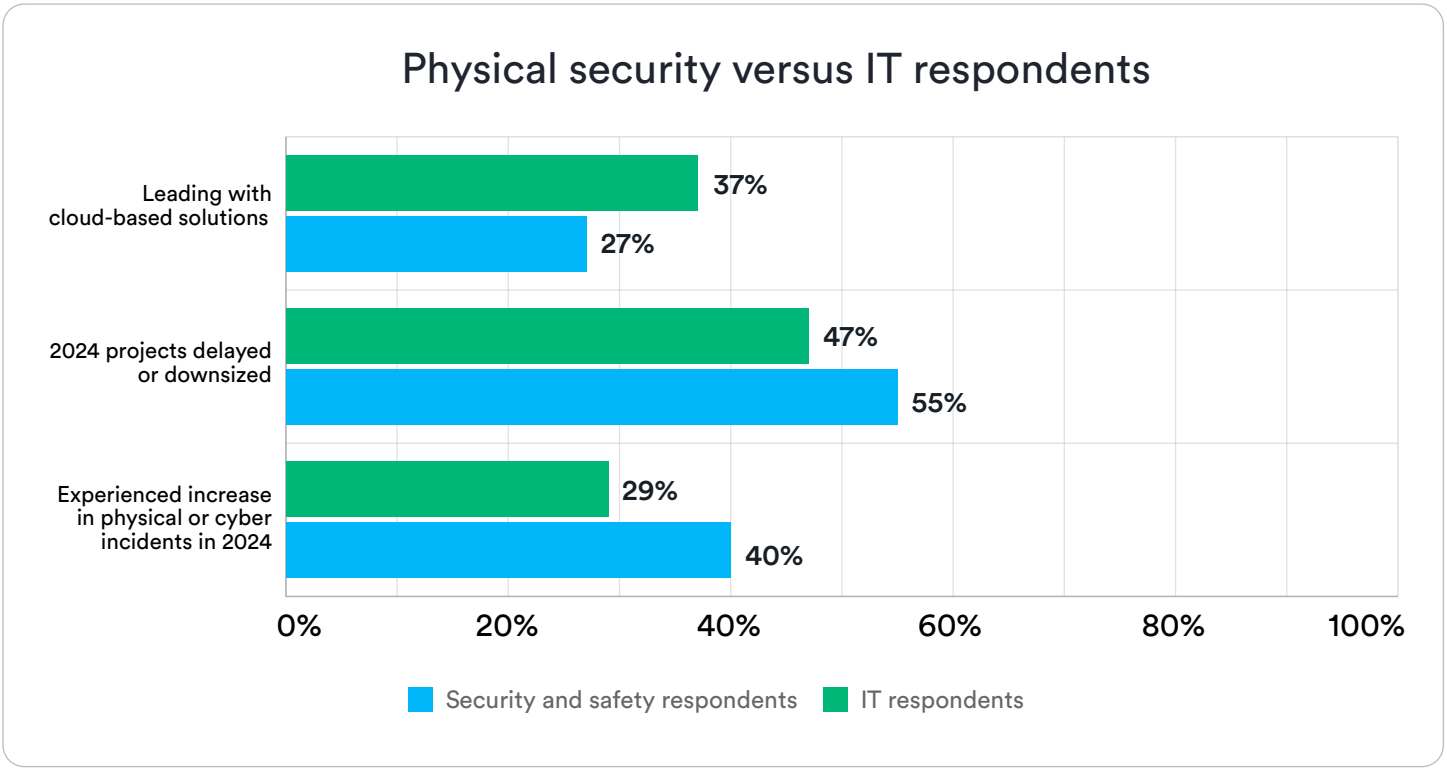


FIGURE P: DISTRIBUTION OF TOP PRIORITIES FOR IT TEAMS VS PHSYICAL SECURITY TEAMS.

Key takeaways

Takeaway 1
Practicality over hype

Coming out of the market uncertainties of 2024, end users are making practical plans for 2025. They're looking for reliable, value-driven solutions that enhance security without introducing unnecessary complexity or costs. The industry-wide focus is shifting to technology that meets day-to-day needs, while they continue to track innovative technology closely to gauge when it is right for them to implement.

The desire to innovate, adopt new technology, and deploy physical security in new ways persists, however, end users are looking for real-world solutions that can reliably improve their work and efficiency within their budget. The move to the cloud and adoption of AI tools remain top of mind but are grounded in business realities resulting in prioritizing hybrid-cloud deployments and a measured approach to finding strong use cases for new technology.

At the heart of priorities and budget, is the ongoing need to build reliable access control and video surveillance systems. These remain the top of mind for physical security departments. Organizations are focusing on ways to adopt new technology into their existing infrastructure to help them improve operations, increase cyber resiliency, and deliver physical security in a more cost-efficient way.

Access control #1

Access control is the top priority for the 5th year running. Projects focused on video surveillance ranked second.

Takeaway 2
IT shapes decision-making

IT's role is to protect digital networks and keep data safe. Physical security protects people, buildings, and other assets. But today these roles are more interconnected than ever. Results of the survey show that this partnership has resulted in greater collaboration with IT in buying decisions.

By combining expertise, these teams work together to the benefit of the organization to navigate the complexities of technology evaluation, and support the many parties involved in the buying process. Together, IT and physical security teams can bring a more complete security approach by combining the threat assessment and response expertise of physical security professionals with IT's specialized skills in network design, data analytics, and cybersecurity. This collaboration strengthens both organizational safety, network security and operational efficiency, creating a more resilient and unified security posture.

50+%

of all respondents say IT departments are involved in purchasing decisions.

Takeaway 3
From cost center to ROI

Physical security data is now commonly shared with IT departments but beyond this, there may be limited knowledge of its contents in an organization. With IT holding the keys to physical security and often system integration requests, physical security department leaders may not fully understand or control the additional organizational value that can be derived from their own systems.

Integrations between security systems, other IoT devices, and operational technologies can fundamentally provide value to business operations. Investment is required to identify problems and explore beneficial integrations and data sources from existing systems. When this concept is embraced it can turn a traditional cost center like physical security into a return on investment when its data is used to drive business decisions. This fact opens the door to the physical security team helping and influencing broader organizational strategy and decision-making.

22%

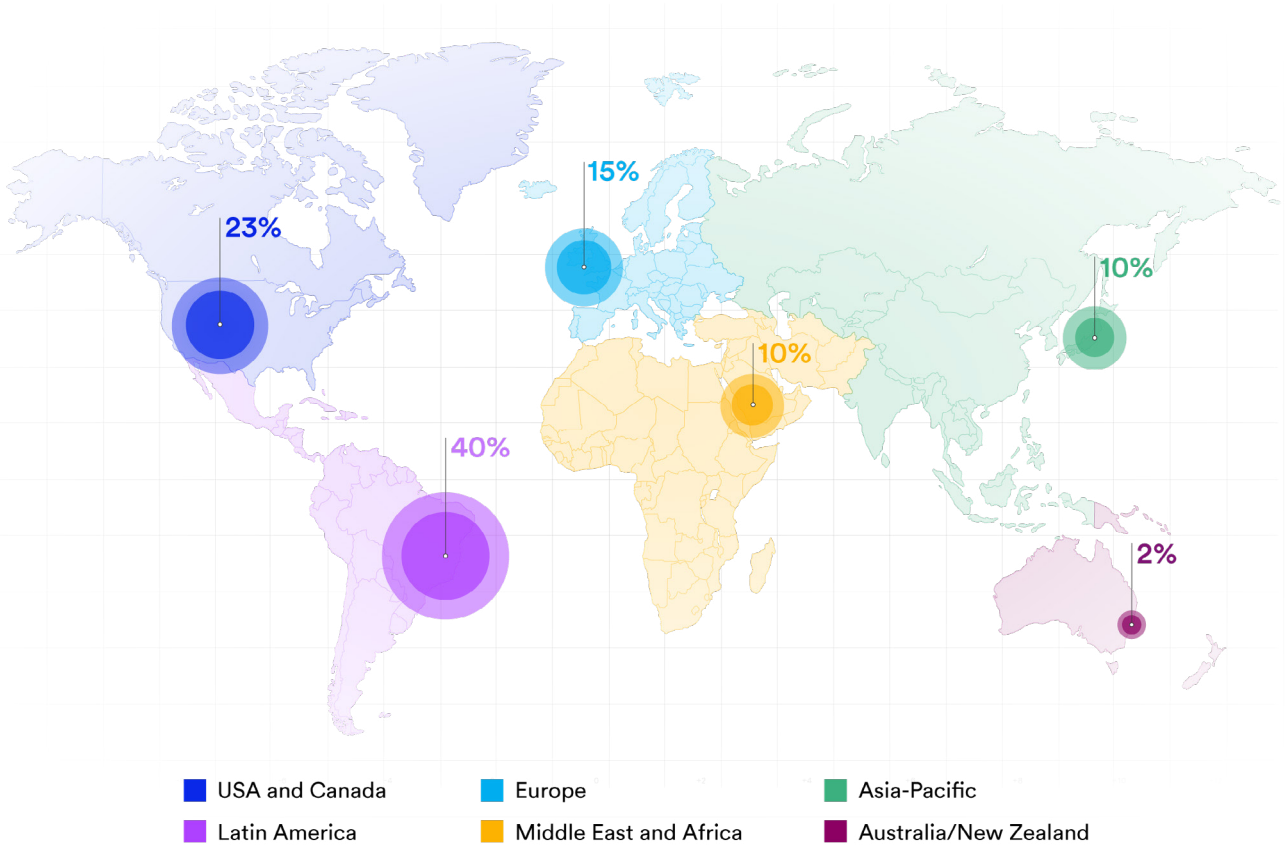
of end users plan to focus on security data access and better reporting in 2025.

Summary of differences around the world

The survey analysis looked at the six following major geographic regions:

- Asia-Pacific
- Australia, New Zealand, and the rest of Oceania
- Europe
- Latin America
- Middle East, Turkey, and Africa
- USA and Canada

This section documents some interesting examples where the survey responses from a given region varied from the global average.



Asia-Pacific

Minimal disruption of 2024 projects, strong cloud and hybrid-cloud adoption in physical security environments.

High hybrid-cloud use in physical security environments: End users from Asia-Pacific reported the highest use of hybrid-cloud overall across all regions. Only 40% of end users describe their physical security environment as entirely on-premises.

Cloud access control: End users from Asia-Pacific had the highest proportion of ACaaS – all cloud access control use and consequently the lowest use of on-premises access control systems.

Most positive story for 2024 project deployments: End users from Asia-Pacific reported the highest portion of 2024 projects which were not impacted by delays. Where there were reported delays, a lower percentage of end users stated this compared with the other regions. End users in Asia-Pacific also reported the highest percentage of projects that had been scaled up (over 20% compared to the global average of 14%).

Australia, New Zealand, and the rest of Oceania

Cloud use is lower due to concerns regarding in-country hosting.

Highest percentage of physical security remaining on-premises: Over 62% of end users stated they were not currently using any cloud in the physical security environment.

Lack of local data center infrastructure in the Australian and New Zealand region is more likely to slow cloud adoption: 21% of end users cited “no data center infrastructure in my region” as a reason for slowing their cloud adoption. The global average was 6% and no more than 8% of end users in any other region selected this reason.

Europe

Mature markets focusing on the replacement of aging systems, intrusion detection popular.

2025 replacement cycle: End users in Europe selected migration and replacement of legacy systems as their #1 focus for 2025. This choice was the 4th most popular on average globally.

Lack of cloud video storage: 55% of end users in Europe stated they would not be storing any video at all in the cloud in 2025. This was significantly above the 33% global average.

Intrusion detection systems more popular in security environments: A higher percentage of European respondents had intrusion detection deployed in their physical security environment – 55% vs 33% global average.

Latin America

Concerns over staffing in the region but most optimistic about future cloud movement.

Staffing challenges in 2025: Channel partners from Latin America were most worried about looming staffing challenges ahead with 88% stating they would increase or greatly increase in 2025. While this figure was high in every region, no other region surpassed a response of 71%.

Most optimistic about future cloud use: Over a quarter of end users from Latin America felt that in 5 years they would have all their physical security systems 100% hosted in the cloud. Only 18% of users globally felt this would be the case.

Less on-premises storage: End users from Latin America had the lowest percentage of on-premises video storage. 33% claimed to mostly store on-premises compared to the global average of 50%.

Middle East, Turkey, and Africa

Big budgets, strong AI implementations but struggling with qualified staff.

Strongest budgets: End users from META were most likely to report an increased 2024 OpEx budget, with 37% stating they had an increase; globally the average was 23%. End users in this region were also most likely to report the largest increases of a 76-100% increase in budget.

Staff training the top challenge: End users from META selected "training and upskilling staff" as their #1 challenge in 2024, no other region selected this challenge as #1.

AI implementations: A greater percentage of end users from the Middle East stated they had already implemented AI in their physical security environment in 2024 or were planning to in 2025 than any other region. A total of 60% of end users versus the global average of 47%. This reflects the advanced nature of some of the enterprise and government projects in the Middle Eastern region.

USA and Canada

More IT involvement and hence a strong focus on cyber security, yet, more cautious on AI use.

Less immediate plans for AI integration: In the US and Canada most end users (57%) stated they had no plans to integrate machine learning, AI, or LLMs in their physical security environments. The global average was 42%. Compared with other regions they were also the least likely to state they had plans to do this in 2025.

Investing in cyber education: 77% of end users in the US and Canada educated employees within their organization on cybersecurity best practices. In other regions it was 66-69%.

Stronger IT involvement: Channel partners found IT departments were involved in the purchasing decision for new physical security systems more commonly in the USA and Canada. 61% of the channel partners found them involved vs 51% on average globally.

Appendix

Appendix 1 – Survey methodology

Genetec Inc. surveyed physical security professionals from August 12 to September 15, 2024.

The goal of the research was to:

- Get a view into physical security operations and environments
- Understand organizations' response to external challenges such as cyber threats and HR difficulties
- Understand the global focus for 2024

Details about the survey and analysis

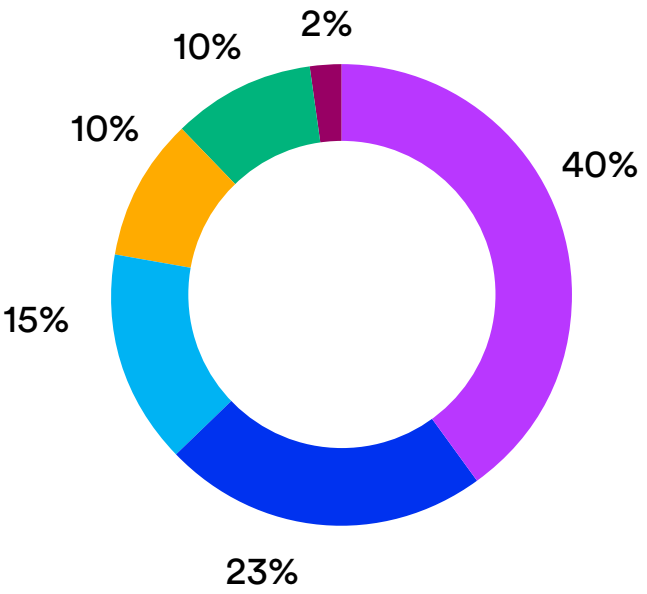
- Following a review of submissions and data cleansing, 5,696 respondents were included in the sample for analysis
- The target population for the survey focused on individuals working for organizations participating in procurement, management, service, and/or use of physical security technology. The target population included Genetec end users as well as participants reached via digital advertising or contacted directly by third parties via their opt-in email lists
- Invitations to take the online survey were sent to potential participants using email in English, French, German, Italian, Spanish, Portuguese, Japanese, and Korean
- The online survey form was available in English, French, German, Italian, Spanish, Portuguese, Japanese, and Korean
- 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 the USA and Canada, Mexico, Central America, the Caribbean, South America, Europe, United Kingdom, Middle East, Africa, East Asia, Southern Asia, South-Eastern Asia, Central Asia, Western Asia, and Australia-New Zealand
- Response rates and survey completion rates varied by region and by organization size potentially introducing sampling errors in sub-sample sets
- Responses were collected from three main target populations: physical security end users, channel partners, and consultants. Data cleansing was performed to validate respondent classification into one of these two populations and limit potential errors. Any non-sampling errors are assumed to result from the collection of data from outside the target population (for example, individuals incorrectly identifying themselves as end users when in fact they are employed as channel partners)

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 all that apply questions, (where respondents can choose multiple answers), percentages refer to the proportion of respondents who selected the individual answer.

Appendix 2 – Survey demographic information

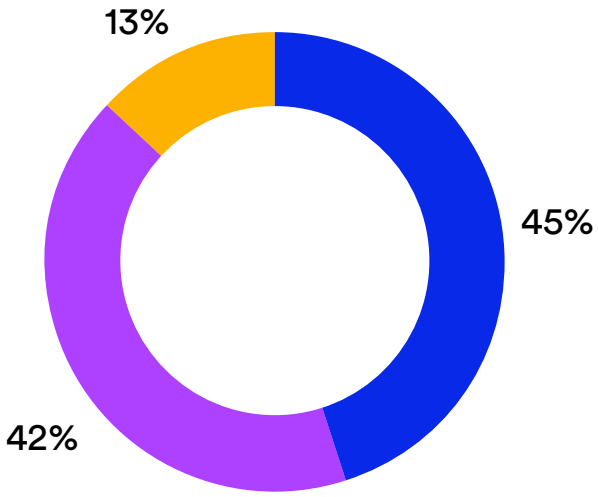
Geographic regions



Latin America	40%
USA and Canada	23%
Europe	15%
Middle East and Africa	10%
Asia-Pacific	10%
Australia/New Zealand	2%

FIGURE 1: RESPONDENTS BY GEOGRAPHIC REGION.

Respondent type



End users	45%
Consultants	42%
Channel partners	13%

FIGURE 2: RESPONDENTS BY ORGANIZATION TYPE.

Appendix 3 – End user demographic information

Job functions

Security and safety	15%
Information technology (IT)	14%
Sales	13%
Engineering, R&D, system design, and quality assurance	11%
Administration/office administration	11%
Customer service or support (technical support)	7%
Operations management	6%
Facilities/operations management	5%
Project management/risk or compliance management	5%
Accounting/finance	5%
Marketing	4%
Purchasing and procurement	2%
Legal	2%

FIGURE 3: END USER RESPONDENTS BY JOB FUNCTION.

Industries

Industrial and manufacturing	17%
Education	14%
Energy, utilities, and telecoms	12%
Transportation	8%
State/local government	8%
Professional services & associations	7%
Retail	6%
Healthcare	6%
Federal/national government	6%
Banking and finance	6%
Sports, gaming, and hospitality	5%
Security systems services	2%
Other	2%
Traffic and parking	2%
Cannabis	0%

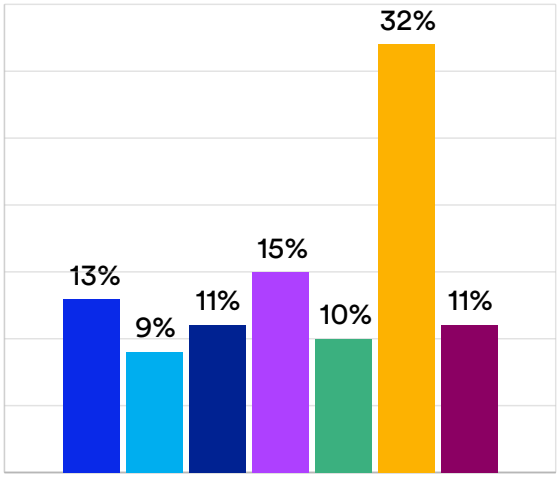
FIGURE 5: END USER RESPONDENTS BY SECTOR.

Employee count

1-20 employees	27%
21-200 employees	24%
201-1,000 employees	21%
1,001-10,000 employees	19%
10,001-100,000 Employees	8%
100,001+ employees	3%

FIGURE 4: END USER RESPONDENTS BY THEIR ORGANIZATION'S NUMBER OF TOTAL EMPLOYEES.

Access control badge holders



	20 cardholders	13%
	21-50 cardholders	9%
	51-100 cardholders	11%
	101-500 cardholders	15%
	501-1,000 cardholders	10%
	1,001+ cardholders	32%
	None of the above/not applicable	11%

FIGURE 6: END USER RESPONDENTS BY TOTAL NUMBER OF ACCESS CONTROL BADGE HOLDERS.

Video surveillance deployment

(# of cameras)

1-9	20%
10-100	27%
101-500	21%
501-1,000	11%
1,001-5,000	13%
5,000+	8%

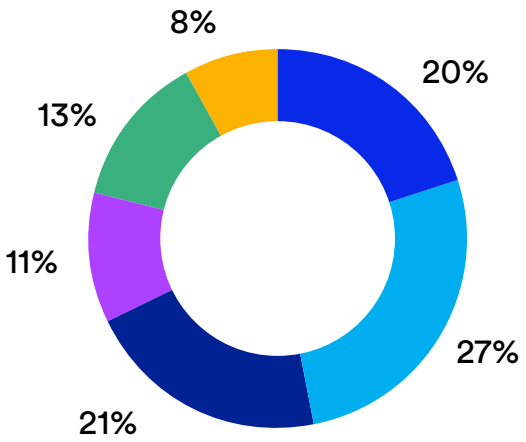


FIGURE 7: END USER RESPONDENTS BY TOTAL NUMBER OF VIDEO SURVEILLANCE CAMERAS DEPLOYED.

Annual revenues (USD)

$500,000-$4.9M	17%
$5M-$24.9M	8%
$25M-$199.9M	7%
$200M-$499.9M	5%
$500M-$999.9M	4%
$1B-10B	6%
$10B+	4%
Unable to disclose	48%

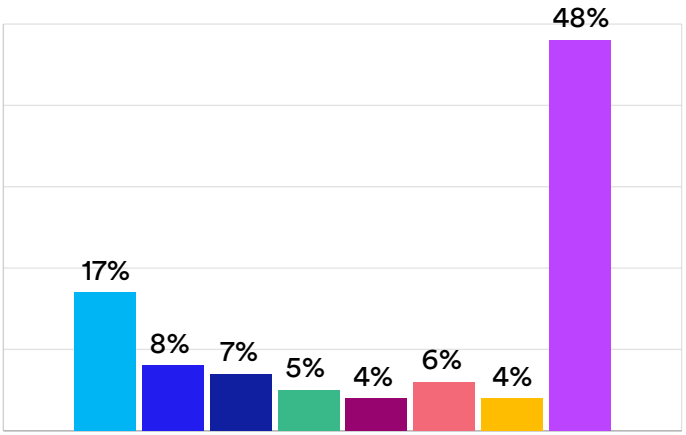


FIGURE 8: END USER RESPONDENTS BY THEIR ORGANIZATION'S TOTAL ANNAL REVENUES (USD).

Employee count (organization's physical security department)

1-20 employees	61%
21-200 employees	25%
201-1,000 employees	9%
1,001+ employees	4%

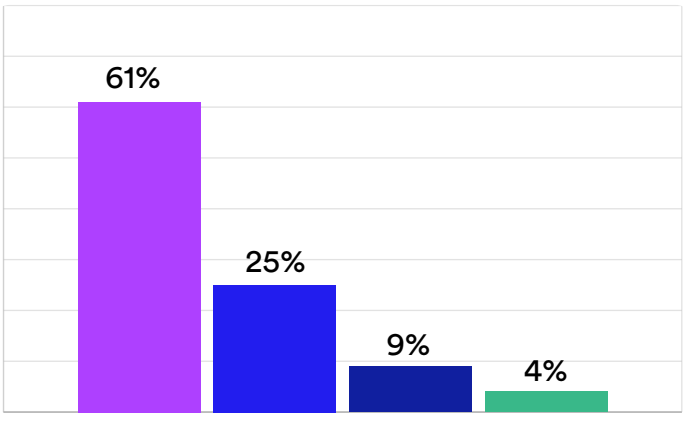


FIGURE 9: END USER RESPONDENTS BY THEIR ORGANIZATION'S PHYSICAL SECURITY DEPARTMENT EMPLOYEES.

Appendix 4 – Open-ended 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?

- Advisory system to retail businesses
- Biometrics
- Customer identification
- Data capture
- Drone detection
- Emergency mass notification
- Escort, bodyguard, reinforced security, armed agents
- Gunshot detection (audio), robots
- Health information system
- Intelligent lighting system
- Invoice management
- Key management
- Logistics
- Road traffic analysis
- Vape, smoke fire
- Video surveillance in fleet of supply trucks, gps, electronic marches
- Wireless duress system

End users and consultants: Do you integrate other functionality (intrusion, perimeter detection, analytics, etc) in this application?

- AI
- Alcohol testing for drivers
- Key management
- Kone elevator, workday
- Line cross, human, vehicle and loitering video analytics
- LPR, event management, etc
- LPR, table games analytics
- Maps of buildings
- PSIM
- Radar
- Robots, gunshot detection, video analytics
- Scada, video analytics, iot
- Workforce geolocation

Channel partners: What is the primary motivation of customers replacing legacy systems?

- Aging
- Bad service and poor system
- Breach of privacy
- Change it because it no longer works
- Compliance to organization's standardization policy
- Comply with new regulations
- Cost
- Eliminating legacy/obsolete systems
- End of life/support/incident
- Esg policy
- Integrator / vendor lock-in
- Internet provider
- Obsolescence

- Product lifecycle
- Reduce downtime
- Speed or capacity increase
- Vulnerabilities on the existing devices/technologies

Channel partners: When selling new physical security solutions to customers, which departments are regularly involved in the purchasing decision?

- Engineering support
- Technology portfolio management
- This is decided on the sales and design side we will include operations to a point

Channel partners: What do you expect could cause project delays in 2025?

- Construction industry is dead in the water, existing customers are slashing budgets
- Government i.R.T. (Re)building permits
- Hiring attractive talent!
- Lack of customer confidence
- Lack of staff on the customer side
- Recession
- War
- Willingness and ability of companies to adopt new technologies

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

- A lot more education is needed for customers
- In fact, it's only now that we're really seeing concrete examples of the use of AI with ROI
- It is confusing the market
- Most asking for AI/ML analytics
- There is a lot of talk about AI, but in security the only evolution that is happening is the increasing deployment of video analytics algorithms on video surveillance devices
- Training is required in order to be able to offer what the client requires
- We're definitely seeing more interest in training and utilization of ai-powered analytics in general. Particularly in video surveillance applications

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

- Accessibility to other data of interest
- Bandwidth
- Compliance
- Connectivity is also an issue parking enforcement is not fully wired
- Driven by infosec
- Long term storage and case sharing
- Network restrictions

End users: What were the top challenges faced by your organization in 2024?

- Acceptance of risks by executives with no esrm processes (i don't think that will happen, so we're not spending money on mitigating it.) With no company/board transparency.
- Accessing data repository
- Alert fatigue
- Audits, redacting system generated reports, incident management and reporting
- Broadcom acquired vmware and pricing increased unexpectedly
- Budgets
- Capital campaign and referendum construction
- Constant it (information security) upgrades, constantly affecting soc systems
- Covid 19
- Decrease in sales
- Doing more with less budget that was almost nothing
- Downsizing corporate re assets/locations.

- Increased budget to accommodate new infrastructure and new 30 employees, from just 6 employes
- Inflation
- Instability of the country for investments
- Managing the perception of safety
- Meeting project timelines and budgets
- Power cuts
- Price of gas - its low
- Security vulnerabilities on old systems
- Timeline of delivery of devices purchased most of the time genetec devices takes about 60 to 90 days delivery
- Unresponsive vendor
- Vendor knowledge

End users and consultants: What new processes or capabilities did you prioritize in 2024?

- Dedicated in house security technician to supplement existing contract with integrator
- Facial recognition
- Obsolescence management
- Unified systems
- Use of drones in security management
- Weapons detection

End users and consultants: What caused the project delays?

- Construction delays
- Decision making issues
- Documentation
- Equipment certification/qualification
- Facilities executives unwillingness to spend budget on recommended risk mitigations, without esrm processes or transparency to company/board
- Finding the right product
- Natural disaster - floods
- Procedural delays
- Product releases
- Project timelines
- Vendor scheduling
- YOY revenue decline

End users: What type of project will be the focus of your department for 2025?

- Upgrade of aging hardware that is at end of service life
- Vape detection

End users: What capabilities do you plan to add to your access control system in 2025?

- Add audio alarm to camera and door alarms
- Fire risk control
- Improve video analytics & AI
- Integrate cctv with access control.
- Integration to hr system
- Jmp journey management plan
- LPR systems for parking capacity management
- Time clock
- Upgrade to osdp protocol and upgrade credentials from prox
- Video analytics integrated to access control to locate tailgating, weapons, etc.

End users: When it comes to cybersecurity, what specific actions/approaches has your organization taken?

- Annual cyber security self-compliance review based on iso 27001
- Closed system only
- Conducting phishing simulation attacks
- Double authentication
- Zero-trust network

End users: What increase(s) in physical security and/or cybersecurity incidents did your organization experience in 2024?

- Death threats
- Deep fake attacks
- Social media threats
- Evolving threat landscape, digital transformation & global instability
- Extended internet outages
- Fake emails
- Hacking
- Uninstalled cameras
- Water damage to equipment

End users: Is your organization leveraging AI tools outside of physical security applications?

- Alexa
- Audiovisual content development
- Automatic chat
- Bi reporting
- Bms smart management (energy efficiency measures)
- Customers' billing, payments, balances
- Human resources, advertising
- HVAC
- Instant messaging
- Internal chat, call management, and data analytics
- Intranet search, company-specific chatgpt
- IT helpdesk
- Marketing and communications.
- Marketing materials
- O365
- Office automation
- Operations
- Our company created an internal gpt system.
- QA, BI, HR
- Start using copilot for office applications
- Watsonx

Consultants: When it comes to your customers which departments are involved in the purchase decisions of security-related products

- Construction project manager
- Health and safety department
- Sales department

Consultants: What were the top challenges faced by the majority of your customers in 2024?

- Acquisitions
- Downsizing and reduced cost initiatives
- Government policies and lack of knowledge

End users and consultants: What new processes or capabilities did you prioritize in 2024?

- Central oversight of multinational facility access control
- Guard tour management
- One card solution
- Risk and threat assessments.
- What kind of projects were affected?
- New installations
- Project due to a change in the threat or a political decision. They become top priority and de facto delay some other projects.
- System integrations

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 increase(s) in physical security and/or cybersecurity incidents did they experience in 2024?

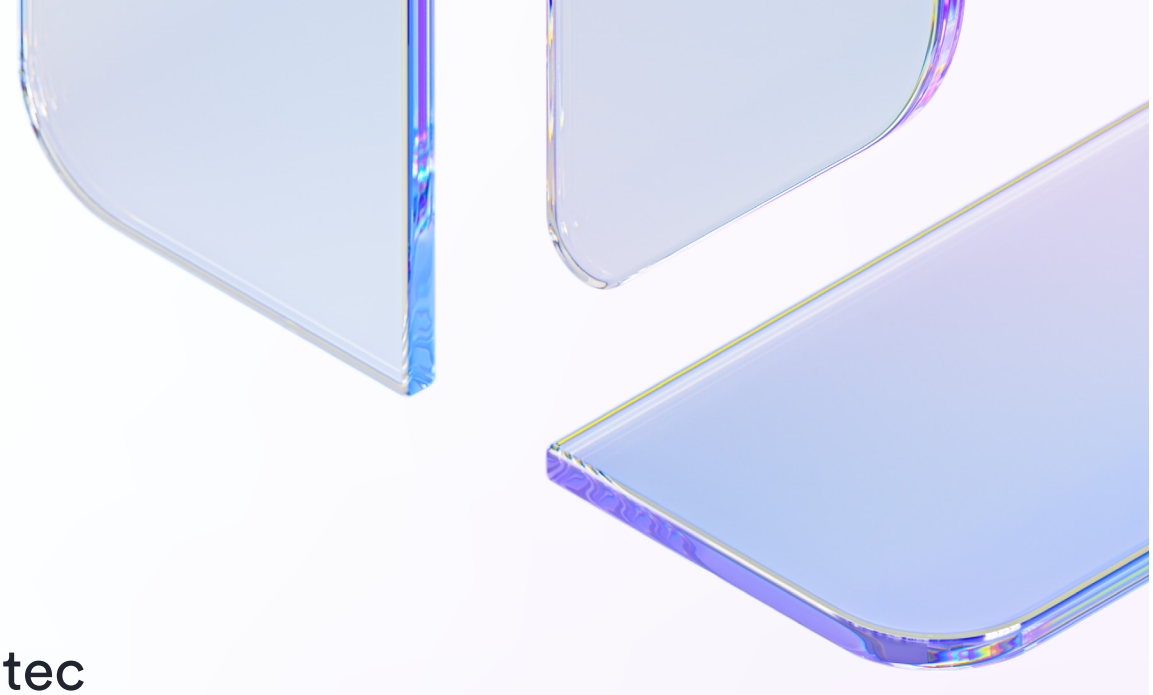
- Arson
- Cloudstrike
- Fights in school
- Fraud
- General probing, testing vulnerabilities
- Impersonations
- Loss of confidentiality of certain personal data
- Protests

Consultants: What kind of data do you feel your clients should collect into their Security Operations Center (SOC) from other systems?

- Documentation
- Insider threat intelligence
- Intrusion and asset monitoring systems
- Outside emergency systems, weather, active shooter, etc.

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

- It has been tremendously helpful with day-to-day repetitive tasks
- Keeping people from thinking it fixes everything
- Need to help clients with risk assessments relating to emerging AI-enabled capabilities of new and existing security products/platforms
- Automate equipment/sensors for business operations and protect universal design
- Mis selling has lead to expectation gaps that we try to reduce
- Reduce noise, use of video analytics, automate tasks, predictions of events



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 while respecting individual privacy.

Based on an open architecture, and built with cybersecurity at their core, Genetec delivers the world's leading products for 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

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

Genetec Inc.
genetec.com/locations
info@genetec.com
@genetec