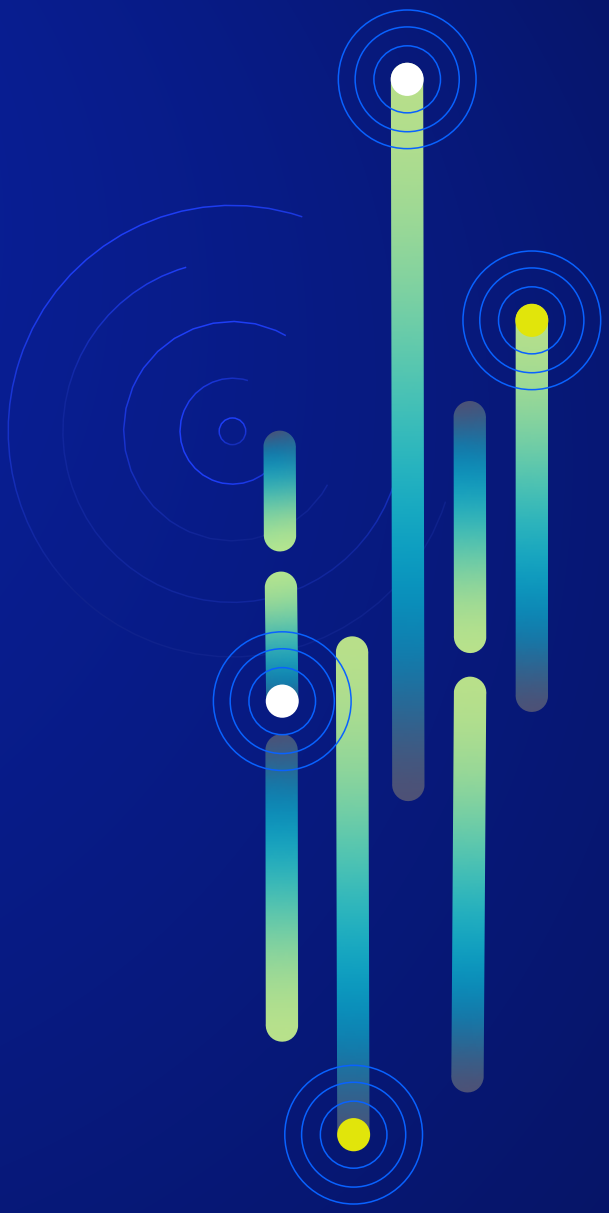
State of Physical Security 2024:

Embracing technology and new ways of working

Research insights from over 5,500 physical security professionals



STATE OF PHYSICAL SECURITY 4TH ANNUAL 2024

Genetec™

Contents

About the research

Genetec Inc. surveyed physical security professionals from August 21 to September 15, 2023. Following a review of submissions and data cleansing, 5,554 respondents were included in the sample for analysis.

Summary of survey methodology

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

End users (EU)

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

Channel partners (CP)

Individuals who consult, install, sell, or service security solutions. For improved readability, this report will refer to channel partners, installers, manufacturers, systems integrators, and providers as channel partners.

The target population was reached through in-person events, and by third parties via 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, installers, manufacturers, systems integrators, and providers. However, some questions were only asked to end users and some only to channel partners, installers, manufacturers, systems integrators, and providers.

Insights

Minor differences were found in results between end users and channel partners responses.

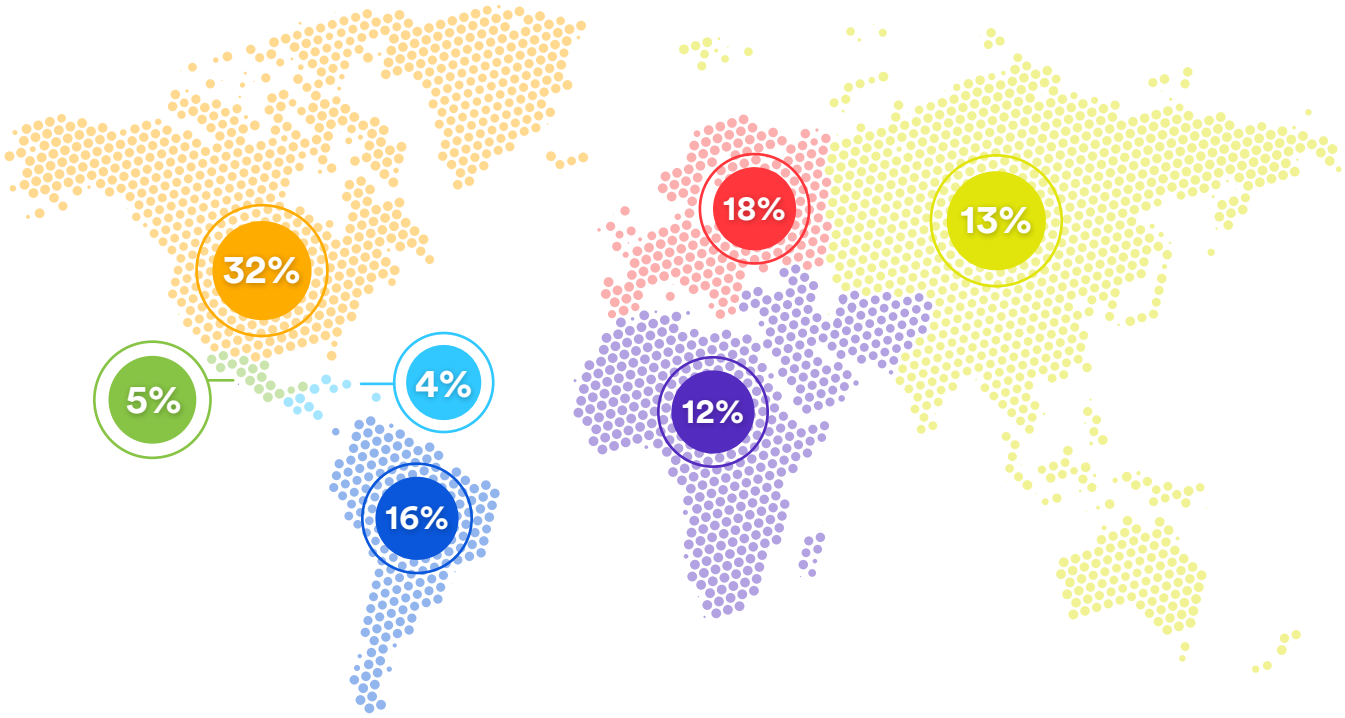
In most cases, there was little difference in the results. Responses from 'end users only' were in line with responses from channel partners, installers, manufacturers, systems integrators, and providers.

This report points out whether answers are from all respondents, end user respondents, or channel partner, integrator, installer, manufacturer, systems integrator, and provider respondents.

Only fully completed surveys submitted by individuals within the targeted population were included in the final analysis.

For improved readability, this report will refer to channel partners, installers, manufacturers, systems integrators, and providers as channel partners (CP).

Target population across all geographic regions



- North America: USA and Canada
- North America: Mexico
- Central America and Caribbean
- South America
- Europe and United Kingdom
- Middle East and Africa
- Asia-Pacific

Only fully completed surveys submitted by individuals within the targeted population were included in the final analysis.

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

Executive summary

It's an exciting time for the physical security industry. Based on the data collected in our 2022 survey, we were surprised by some of the results from the 2023 survey. From the increased demand for cloud and technology to the challenges that did not improve as expected–it's clear that the industry is embracing change and adapting to new ways of working.

New technology is being quickly adopted

The integration of new applications in physical security environments has increased and does not show signs of slowing down in the year ahead.

Cloud connectivity accelerates

Adoption of the cloud in the physical security industry has been gradual but is now accelerating. The future for most physical security solutions appears to be a blend of on-premises and cloud-based solutions.

Cybersecurity concerns increase

Despite implementing processes to face cybersecurity challenges, the level of concern about cyber threats continues to rise.

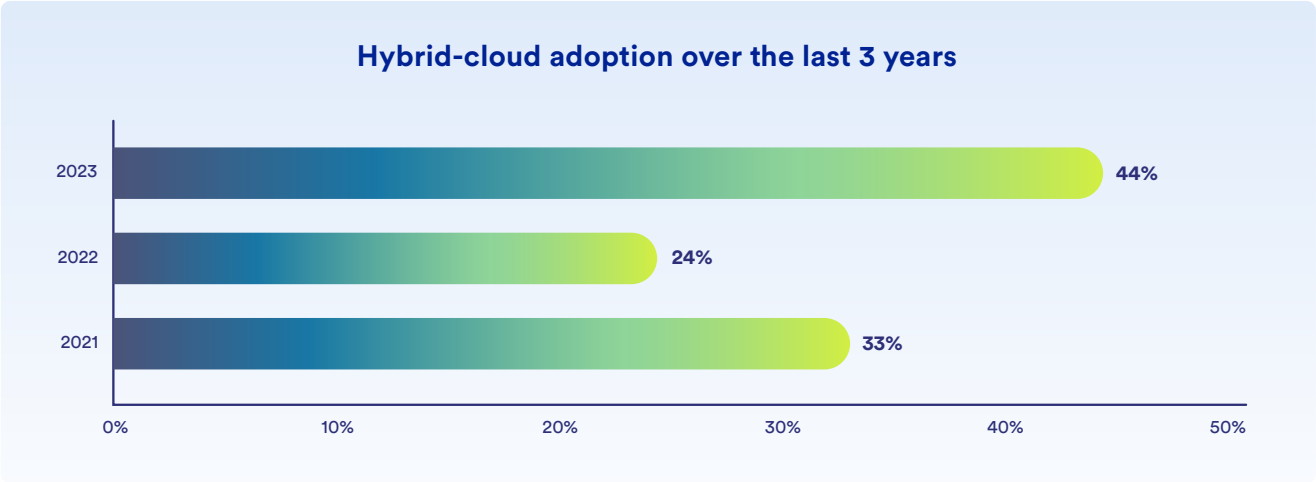
Supply chain and HR challenges linger

Supply chain constraints and human resource (HR) issues related to the pandemic were expected to be resolved by now. However, these challenges continue to disrupt many organizations.

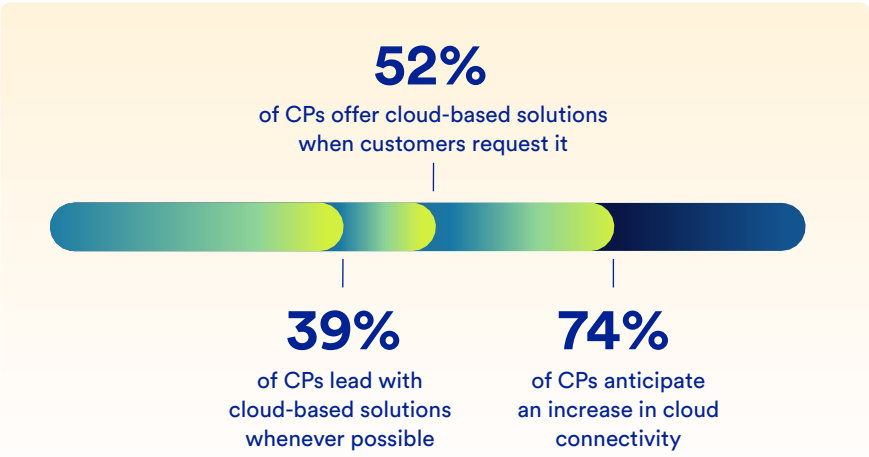
Global key findings

Speeding towards the cloud

Over the past decade, the adoption of cloud for physical security has been gradual. However, it's now accelerating. In the 2023 survey, 44% of end users indicated that over a quarter of their physical security environment is cloud or hybrid-cloud compared with 24% in the 2022 survey.



Despite the move to the cloud, hybrid architectures blending on-premises and cloud-based solutions will suit most organizations. This move to hybrid systems is already underway.



Insights

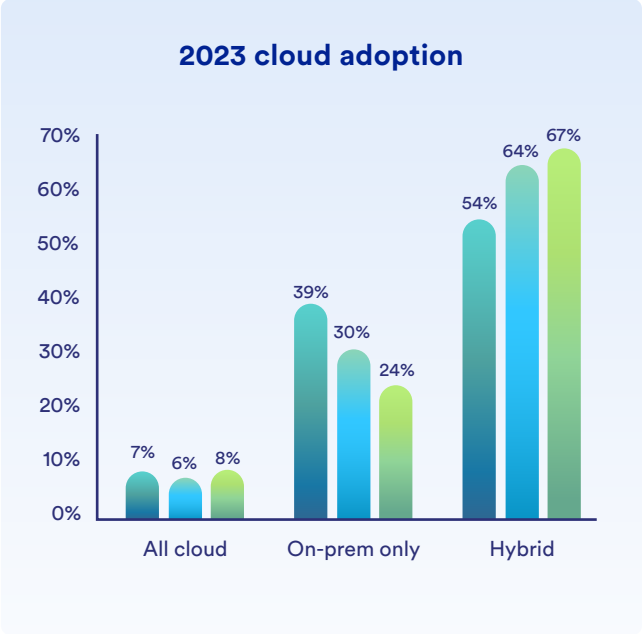
2023 survey data indicates an 11% increase in hybrid-cloud video storage.

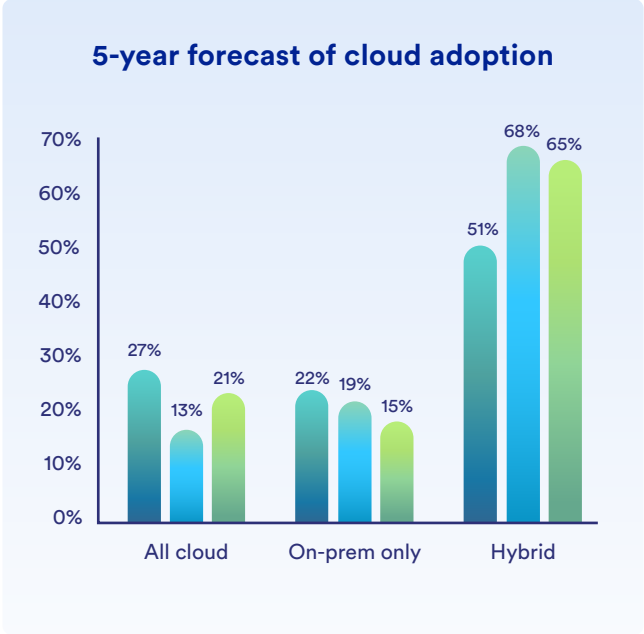
Cloud adoption by organization size

Cloud-based video surveillance systems were initially adopted fastest by both small and larger organizations that had distributed sites and a small number of cameras, such as fast food restaurants and retail bank chains. Results from 2023 indicated that this is changing. A greater number of large enterprise organizations that have over 100,000 employees are now adopting cloud-based video surveillance systems.

Insights

36% of end users from state and local government and 29% from justice and public safety reported that no solutions would be hosted in the cloud.





1-200 employees 201-10,000 employees 10,001+ employees

The move to the cloud is hybrid

In our 2022 survey, respondents reported that 58% of their physical security system was on-premises and 42% was cloud or hybrid-cloud. In our 2023 survey, those numbers jumped to 33% of respondents stating that their physical security systems were on-premises and 67% were cloud or hybrid-cloud. These results indicate that end users don't want to be locked in and are seeking options when leveraging cloud technology to optimize their infrastructure.

"By utilizing cloud solutions, we can leverage the expertise of cloud service providers' professional teams to monitor and maintain our physical security applications, thereby alleviating the burden on our internal teams."

–End user respondent

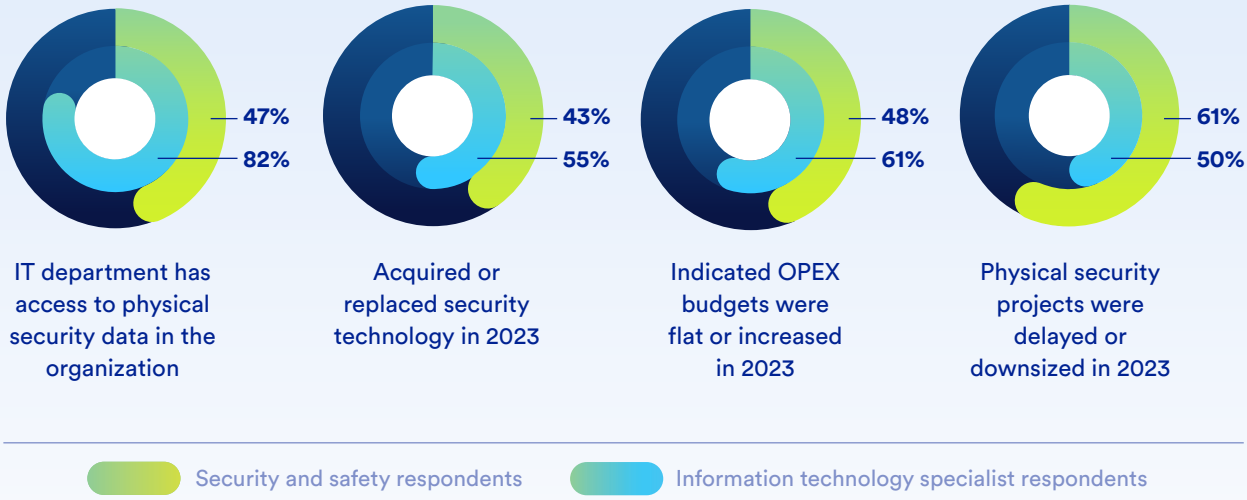
Security and safety specialists compared to IT specialists

A decade ago, most physical security systems in larger organizations were managed by teams in specialized security departments. The transition to network physical security systems has meant that information technology (IT) departments are taking greater responsibility for managing physical security systems as part of their technology governance. These departments can have different outlooks and priorities. This explains why respondents who identified their job function as "information technology" often had a different point of view than their counterparts who selected "security and safety".

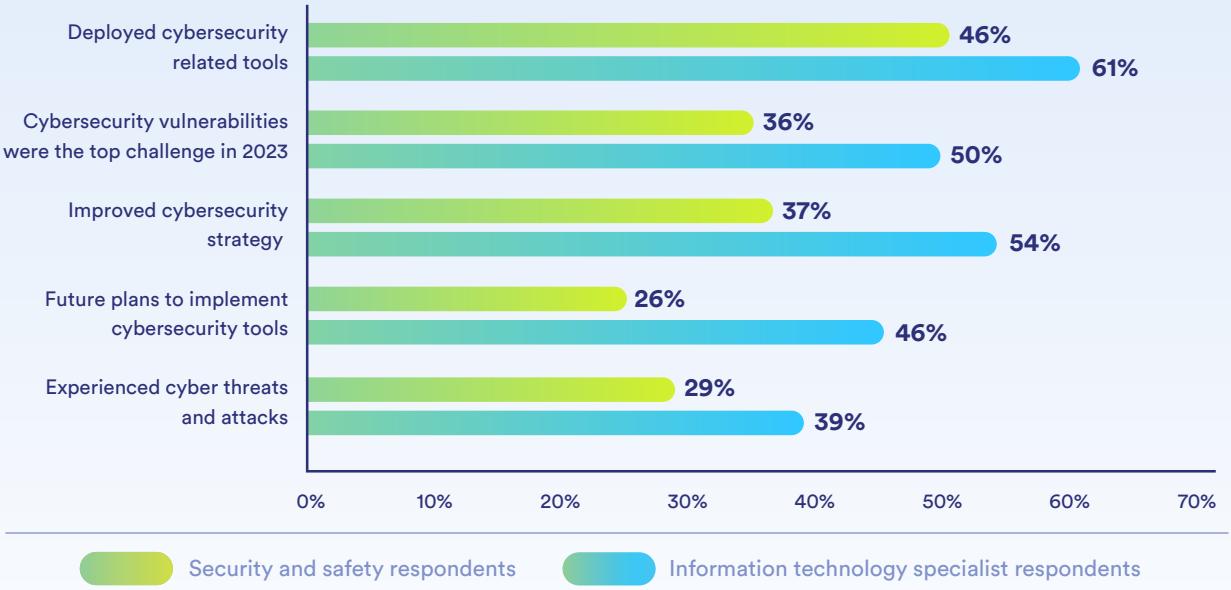
Insights

Cybersecurity issues were prioritized in the responses of "information technology" respondents. The survey data also indicates that they have higher budgets compared to other departments which could make it easier to focus on cybersecurity measures.

Security and safety vs information technology



Perspective of security and safety compared to IT on cybersecurity



Viewpoint

Many organizations still handle video and access control separately. However, there is a strong push for modernization, encouraging these organizations to break down their systems and technology silos. Some even have different departments, so there is an organizational design issue as well. Collapsing these silos requires both strong leadership and effective management. It is not just about the technology; how it is managed and led is just as important.

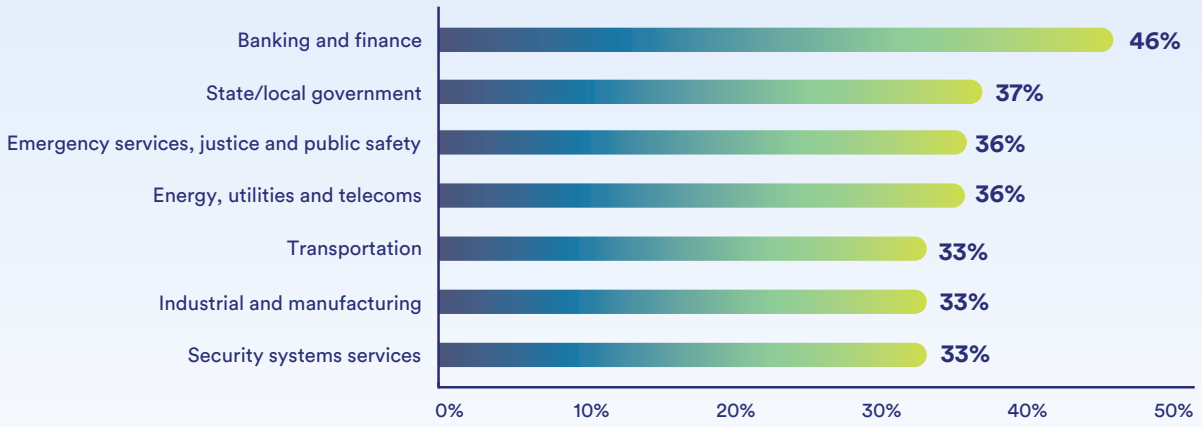
"Technology changes quickly, but organizations change much more slowly."– George Westermen

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

Concerns over cyber threats increase

A concerning 31% of end users indicated that their organization was targeted by cybercriminals in 2023.

Industries most affected by cyber threats



Organizations prioritize a better cybersecurity strategy

In response to cyber threats, 42% of organizations increased deployments of cybersecurity-related tools in their physical security environments in 2023, up from only 29% in 2022.

Cyber concerns about the cloud decrease

In the 2022 survey end users ranked cybersecurity risks as the top reason for deterring their organization from adopting cloud solutions. In the 2023 survey, this dropped down to 6th place, indicating that attitudes are changing rapidly.

Top 5 actions being taken by CPs to improve cybersecurity

61%
Educating users on cybersecurity best practices

47%
Hardening security infrastructure

42%
Fine-tuning user permissions and privileges

42%
Protecting the system from unauthorized access

41%
Securing data storage

Viewpoint

“

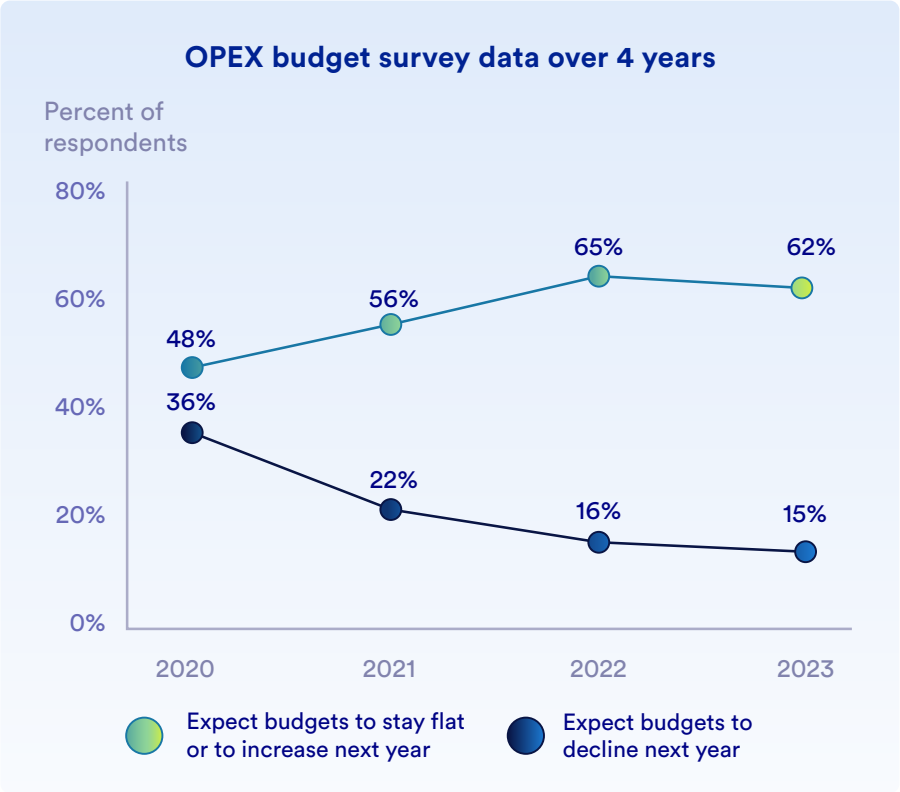
With the rise of cyber risks in physical security systems, organizations are showing a heightened awareness of cybersecurity and adopting best practices to confront these challenges head-on.

This mirrors the pattern observed during the early stages of cybersecurity integration in the IT industry. As IT professionals increasingly engage in physical security projects, their expertise is enriching the field. The physical security industry is heading in the right direction, but there is still some distance to cover.

Mathieu Chevalier
Manager and Principal Security Architect, Information Security
Genetec Inc.

OPEX budgets continue to rise

The good news for the industry is that OPEX budgets continue to grow. 62% of end users expect budgets to increase or remain flat into 2024 and only 15% expect budgets to decline. These are very similar proportions to those expected by respondents for the year ahead in our 2022 survey. In 2022, the market for video surveillance equipment boomed in many regions, with market analysts Novaira Insights reporting growth of 19% in the Americas and 12% in EMEA.



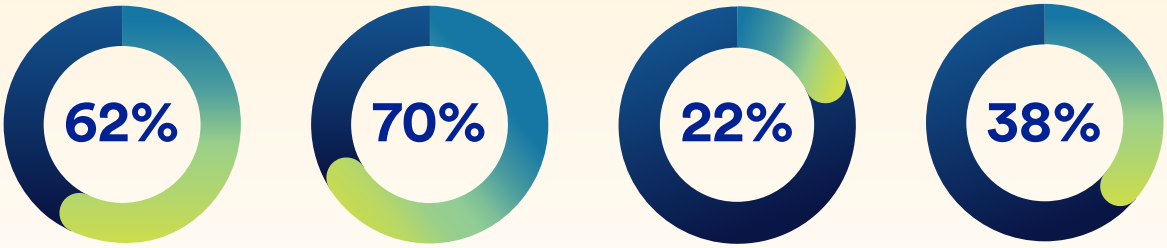
Insights

Many cloud solutions are charged on a recurring basis. A case could be made for the increase in OPEX budgets being partially tied to the growing interest in, and adoption of, cloud and hybrid-cloud solutions. This might also be reflective of the IT departments' ongoing influence on the purchase of physical security solutions.

HR challenges get worse

Across all industries, talent shortages, back-to-the-office plans, and employee expectations for new ways of work challenged organizations over the last couple of years. Unfortunately, the results from our survey suggest that for channel partners, HR challenges are getting worse rather than better.

Distribution of HR challenges according to CPs



HR problems increased in 2023

HR problems will increase in 2024

HR problems will remain the same in 2024

Labor shortages will cause project delays in 2024

38%

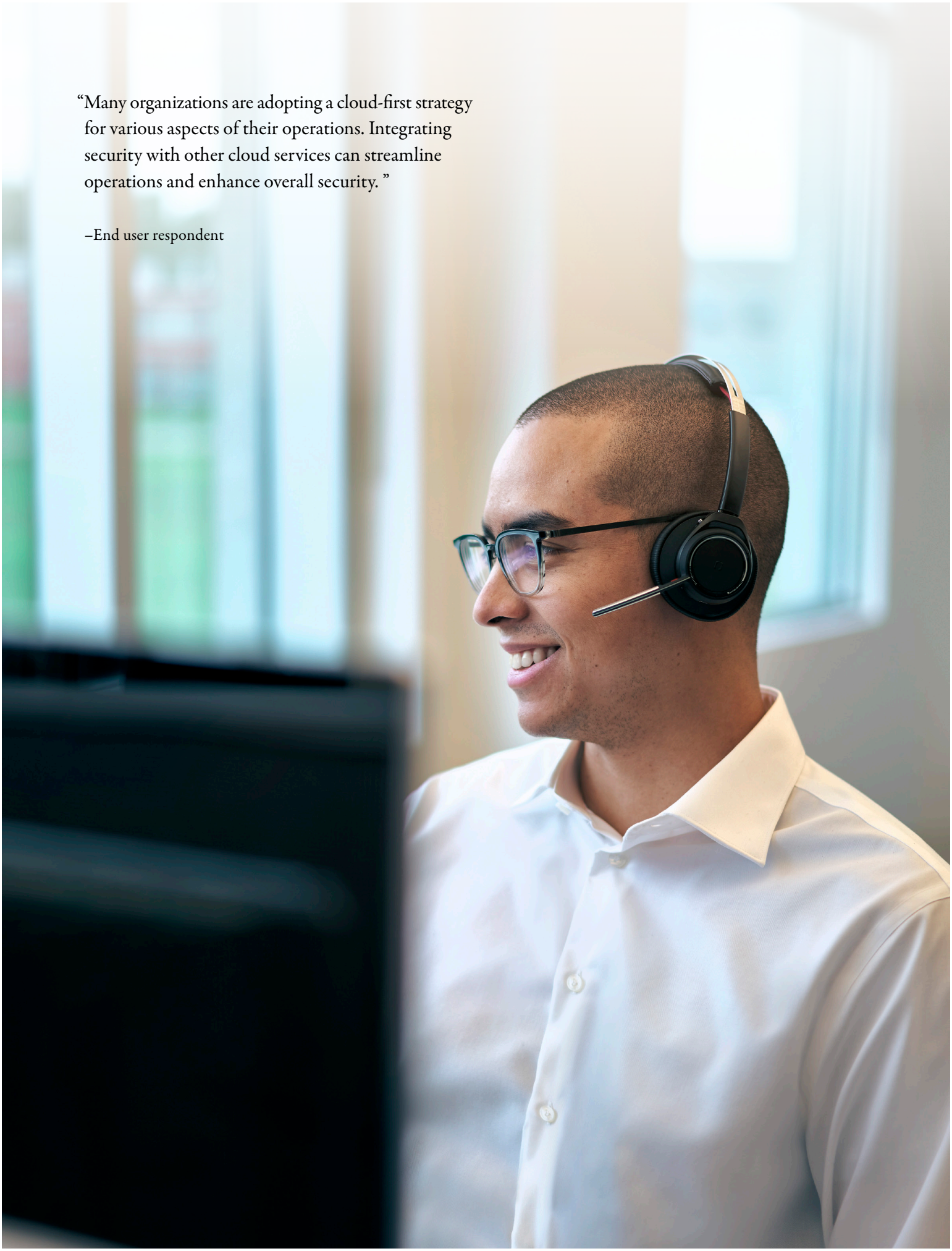
Similarly, 38% of end users are having issues attracting talent and another 38% stated they are also experiencing labor shortages.

Viewpoint

“

As technology adoption evolves it opens up opportunities for the whole industry. New approaches to work and feature sets powered by greater connectivity and hybrid cloud delivery can facilitate greater scalability, security, and agility in physical security deployments in the years to come. This means end users can work with their partners to adapt their integrations to fit their exact needs to benefit from innovation.

Michel Chalouhi
Vice-President of
Global Sales
Genetec Inc.



"Many organizations are adopting a cloud-first strategy for various aspects of their operations. Integrating security with other cloud services can streamline operations and enhance overall security."

–End user respondent

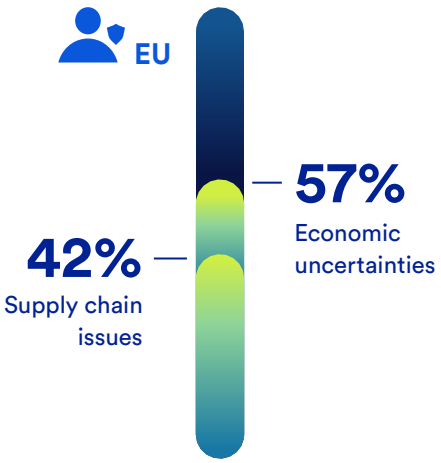
Supply chain issues linger

Many physical security projects were delayed in 2021 and 2022 due to unprecedented supply chain problems. These delays have persisted into 2023.

45% of end users responded that their physical security projects had been delayed or downsized in 2023. An additional 12% confirmed they had been canceled altogether.

56% of channel partners responded that they had a deployment backlog at the start of 2022. 50% believe supply chain issues will greatly increase or somewhat increase. While the remainder believe it will stay the same (28%) or somewhat decrease or greatly decrease (22%).

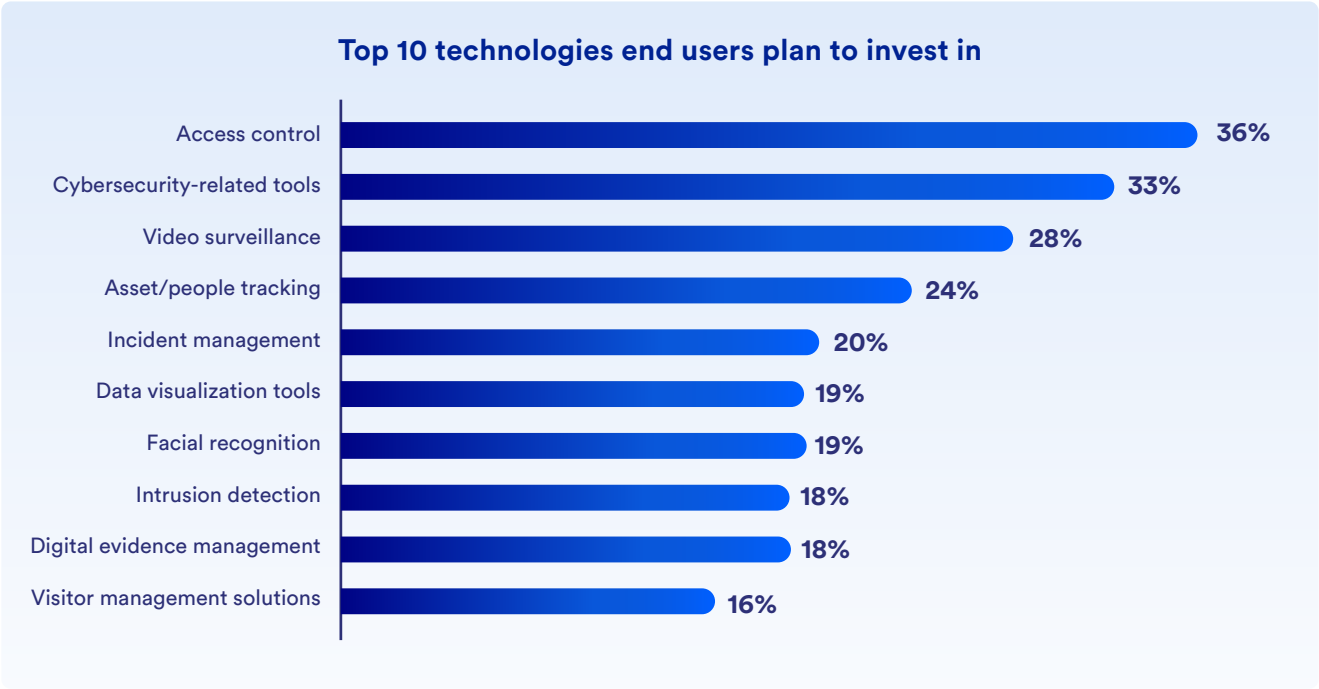
Top reasons for project delays



Note: Respondents could select more than one reason

New technology is embraced

Advances in technology are being applied to physical security environments to enhance traditional security offerings. In our survey, end users were asked what type of projects they plan to focus on for 2024. Along with traditional physical security projects like access control, video surveillance, and intrusion detection, a relatively high proportion of end users selected these technologies as well:



Artificial intelligent integrations on the rise

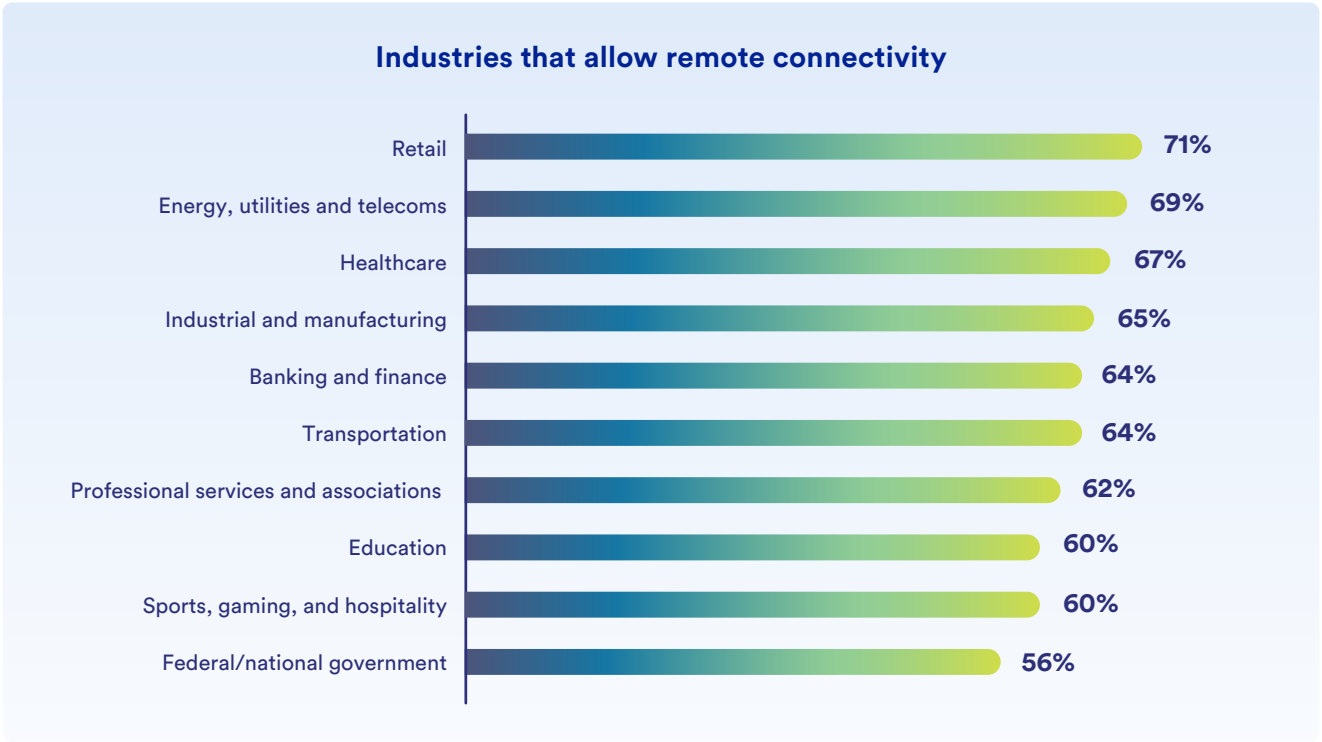
22% of end users stated that their organization had already integrated machine learning, artificial intelligence (AI), and/or large language model (LLM) applications in their physical security environment. This varied by industry with 46% of respondents in the traffic and parking sector indicating they had adopted AI, while only 10% did in the healthcare industry.

Insights

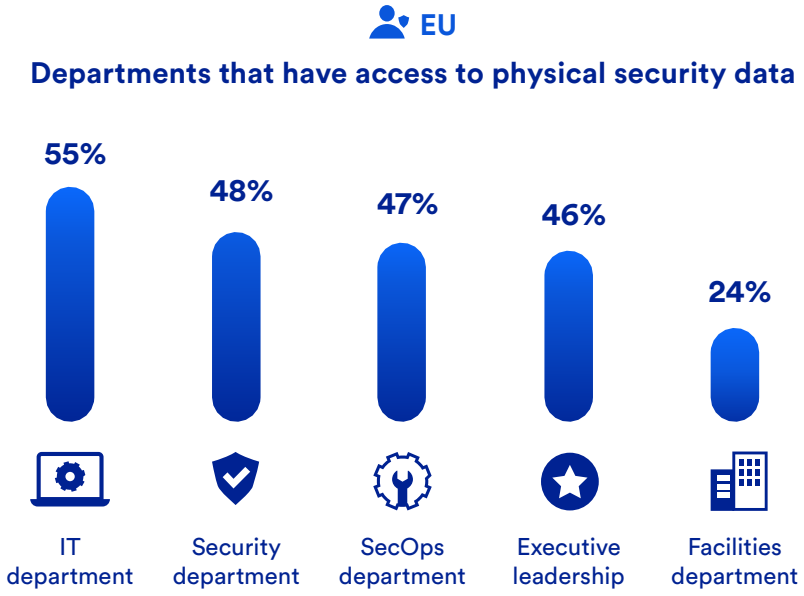
33% of end users have plans to add AI applications in 2024.

Connectivity

64% of end users responded that their organization's current physical security system allows remote connectivity from outside of their local network (e.g. remote firmware updates, patches, remote monitoring, etc.). For the organizations where this is not the case, 31% of end users indicated there is a current plan to enable remote connectivity from outside their local network. The survey data varied considerably by sector.



55% of end users stated that their information technology (IT) department has access to physical security data. Given the surge in technology and cloud adoption, it's not surprising that IT departments are playing a bigger role in physical security. Their skills are often required to securely integrate new applications into relevant organizational networks. Collaborating further has become essential to ensure appropriate selection, governance, and cyber resilience of networked physical security solutions.



Viewpoint

With 1) the current hybrid work movement changing the labor force's landscape, 2) a supply chain that is still experiencing some instability and uncertainty, 3) an ever-growing focus on digital transformation, 4) the leapfrog advancements in machine learning, and 5) the shift towards greater cloud connectivity, the physical security industry is in a period of challenging but exciting changes. These changes are translating into tremendous opportunities for industry players that are able to act on them quickly and adapt to this changing environment to bring data-driven innovative solutions to the forefront for their partners and customers alike. The ability for organizations to adapt is becoming one of the most important capabilities for any enterprise to succeed.

Nadia Boujenoui
Vice-President of
Customer Experience
Genetec Inc.

Key takeaways

1

New confidence in the cloud

The physical security industry is catching up to other industries in its adoption of the cloud. From the responses received to cloud questions in this year's survey, we noted that end users have come to understand its value. Where they once ranked cybersecurity risks as a top deterrent for moving to the cloud, there is now more knowledge and confidence.

Hybrid-cloud deployments seem to be the direction for most organizations as they can rationalize the costs, concerns, and approaches to migrating to the cloud.

2

Emergence of tech savvy physical security and IT teams

As the adoption of cloud-based physical security systems surges, so do cybersecurity threats, data management, and compliance requirements. It's no surprise that IT and physical security teams have started to work together more closely.

The 2023 survey indicates a surge in new technology integrations. End users have more confidence in using these applications to improve physical security insights and operations. The result of more IT involvement.

As more technology is adopted and remote connectivity from outside local networks increases, the relationship between IT and physical security will continue to evolve.

3

Making cybersecurity a top priority

The physical security industry's response to cyber threats in the past has generally been inadequate. However, attitudes are changing. Several survey questions revealed a greater focus on cybersecurity for both end users and channel partners. This could be in response to an increasing number of respondents admitting their organization has faced cyberattacks.

Information technology (IT) respondents prioritized cybersecurity in several of their responses. They also appear to have larger budgets which might make it easier for them to focus on maintaining and funding a cybersecurity strategy.

44%

of end users indicated that over a quarter of their physical security environments are cloud or hybrid-cloud in the 2023 survey. This compares with 24% in the 2022 survey.

55%

of end users indicated that the IT department has access to physical security data.

42%

of end users indicated their organization deployed cybersecurity-related tools in their physical security environment in 2023.

Summary of differences around the world

The survey data did not vary statistically from the global average and mostly demonstrated a common view, experience, and expectation in the majority of cases.

The greatest variance was often in the three Latin American regions Mexico, Central America and the Caribbean, and South America. For other regions, we have also documented the rare instances where we saw significant differences in responses from the global average.

Asia-Pacific

Deployment backlog and focus on cybersecurity tools

Deployment backlogs: 41% of channel partners reported experiencing deployment backlogs at the start of 2023. A contrast to the global figure of 56%. This indicates a more streamlined approach to deployments in the region.

Connectivity and remote access: 57% of end users indicated that their organization's physical security system allows remote connectivity. A total of 65% of channel partners in APAC indicated that over 25% of new physical security systems they deploy will be cloud or hybrid-cloud in the next five years, compared to 69% of channel partners globally.

Focus on cybersecurity: 42% of end users indicated that their departments would focus on implementing cyber-related tools in 2024, compared to the global average of 33%. This emphasis on cybersecurity aligns with the fact that 50% of end users identified cybersecurity vulnerabilities as a top challenge for their organizations in 2023, compared to 36% globally.

Central America and the Caribbean

Focused on system unification and cybersecurity

Slower cloud adoption: Cloud adoption in this region seems to be growing at a slower pace than in other countries. A smaller percentage of channel partners in this region (37%) have clients using cloud security compared to the global average (49%). Additionally, 55% of channel partners in this region indicated that 25% of the physical security systems they deploy will be cloud or hybrid-cloud in five years, compared to 69% of channel partners globally.

Staffing challenges: Staffing seems to be a big issue in Central America and the Caribbean, with 80% of channel partners in the region expecting challenges in 2024. This surpasses the global average of 70%.

Deployment backlog: In 2023, 71% of channel partners in this region started the year with project backlogs compared to the global average of 56%. Also, a higher percentage (84%) experienced an increase in their backlog during the year, exceeding the global figure (61%).

Delays and causes: Economic uncertainties are less frequently cited as a reason for project delays, with only 45% of end users in this region choosing this option, compared to the global average of 57%.

Combining video surveillance and access control: End users in Central America and the Caribbean are more enthusiastic about unifying video surveillance and access control than other regions. Among end users who have both systems, 68% integrate or unify these solutions, whereas globally, this figure stands at 56%.

Cybersecurity focus: While other regions prioritize investment in cybersecurity-related tools, only 23% of end users in this region indicated that these tools will be a departmental focus in 2024, compared to the global average of 33%. However, the region excels in user education on cybersecurity best practices, with 77% of respondents reporting their organization's efforts in this area, exceeding the global average of 61%.

Europe, United Kingdom, Middle East and Africa (EMEA)

Slower shift to the cloud and delays amid global conflicts

Cloud transition: Survey data from EMEA indicated this region is the slowest to shift to cloud-based solutions. A total of 62% of channel partners indicated that over ¼ of new systems they deployed will be cloud or hybrid-cloud in the next five years, as compared to the global average of 69%.

Talent retention: In EMEA, keeping talent is less of a problem than in other regions. Only 33% of end users stated that talent retention was a challenge in their department in 2023, as opposed to the global average of 39%.

Impact of global conflicts: More end users in EMEA (15%) cited war or conflict as the main cause of project delays, significantly exceeding the 8% global average. This emphasizes the influence of geopolitical factors on project timelines in the region.

Mexico

Resilient to supply chain issues and enthusiastic about the cloud

Supply chain resilience: Respondents from Mexico demonstrate remarkable resilience in addressing supply chain challenges. A lower percentage of end users in Mexico indicated that supply chain issues caused project delays in 2023 (27%) than globally (42%). This suggests a more optimistic outlook despite global concerns.

Cloud adoption: Respondents in this region display a stronger interest in cloud-based security solutions than other regions. 85% of channel partners anticipate an increase in end user customers adopting cloud connectivity for security in 2024, exceeding the global average of 74%.

Stable operational budgets: Fewer end users (15%) saw their OPEX budget increase in 2023 compared to the global average (29%). Additionally, more end users from this region (47%) anticipate a consistent OPEX budget in 2024, exceeding the global rate (35%).

Cybersecurity priorities: Unlike other regions that are focusing on strengthening their cyber-security strategy, respondents from Mexico stand out with a lower percentage of end users (19%) who prioritize cybersecurity-related tools in their 2024 departmental focus, compared to the global average (33%).

South America

Cloud growth and ongoing HR and economic uncertainties

Cloud growth: Survey respondents in South America have an optimistic outlook on cloud technology in their region. A higher percentage of channel partners (83%) expect an increase in the adoption of cloud-connected security systems in 2024, exceeding the global average (72%). As for end users, a lower percentage indicated that over 25% of their organization's physical security environment is cloud or hybrid-cloud (29%) than globally (44%).

Human resource challenges: Channel partners are particularly concerned about staffing challenges, with 83% expecting this issue to rise, compared to the global average of 70%.

Supply chain: Fewer end users in South America (30%) faced project delays due to supply chain problems in 2023 compared to the global average (42%). On the other hand, more channel partners in South America (51%) expect prices to somewhat drop as supply chain issues improve in 2024, while globally, fewer than 39% indicated the same.

Budget and project delays: Only 15% of end users reported higher 2023 budgets, which is less than the global average of 29%. Project delays are mainly due to economic (70%) and political (36%) uncertainties, which are higher than the global averages (57% and 25%, respectively). Also, economic uncertainties and inflation are perceived as potential culprits for project delays in 2024, with 59% of channel partners in South America expressing concern, compared to the global average of 48%.

Cybersecurity approach: South America takes cybersecurity seriously, but surprisingly only 35% of end users identified hardening security infrastructure as a specific approach taken by their organizations, in contrast to the global average of 47%.

USA and Canada

Cloud adoption and supply chain challenges

Cloud connectivity: Channel partners in the USA and Canada are ahead of the curve when it comes to cloud adoption, with 61% of them reporting that over a quarter of their existing end user customers allow cloud connectivity for security. This percentage surpasses the global average of 49%.

HR challenges: Unlike the global trend where HR challenges such as training and upskilling are common, only 36% of end users in the USA and Canada identified these as issues in their departments. This percentage is lower than the global average of 46%.

Supply chain issues: Project delays due to supply chain issues are a bigger problem in the USA and Canada, with 55% of end users concerned. Globally, a lower percentage (42%) faced these delays.

Appendix

Appendix 1 – Survey methodology

Genetec Inc. surveyed physical security professionals from August 21 to September 15, 2023.

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

Following a review of submissions and data cleansing, 5,554 respondents were included in the sample for analysis.

Details about the survey and 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, Dutch, Italian, Spanish, Portuguese, Japanese, and Korean.
- The online survey form was available in English, French, German, Dutch, 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 two main target populations: physical security end users and channel partners, installers, manufacturers, systems integrators, providers. 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

Genetec Inc. surveyed physical security professionals from August 21 to September 15, 2023.

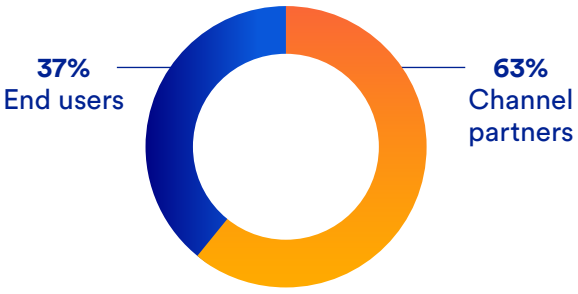
Industries

Channel Partners (CPs, installers, manufacturers & consultants)	63%
Industrial & manufacturing	6%
Energy, utilities and telecoms	4%
Education	4%
Transportation	3%
Healthcare	3%
Other	2%
Professional Services & Associations	2%
Banking and finance	2%
Federal/National Government	2%
Sports, gaming and hospitality	2%
Retail	2%
State/Local Government	2%
Emergency services, justice and public safety	1%
Security Systems Services	1%
Traffic and parking	1%
Cannabis	0%

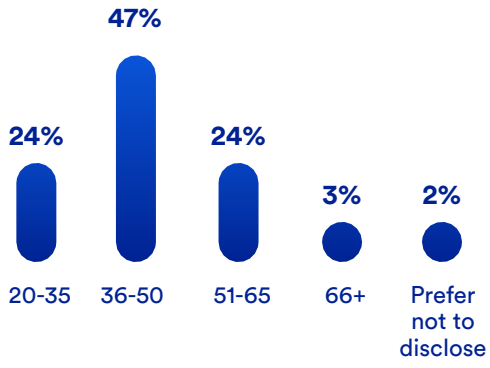
Job functions

Engineering, R&D, System design & quality assurance	15%
Security & Safety	13%
Information technology (IT)	12%
Sales	10%
Administration/office administration	8%
Operations management	7%
Project management/Risk or compliance management	7%
Customer service or support (technical support)	6%
Facilities/operations management	6%
Administration/ legal	4%
Accounting/Finance	4%
Marketing	3%
Quality management	2%
Estimator	2%
Purchasing and procurement	1%
Legal	1%

Respondent type

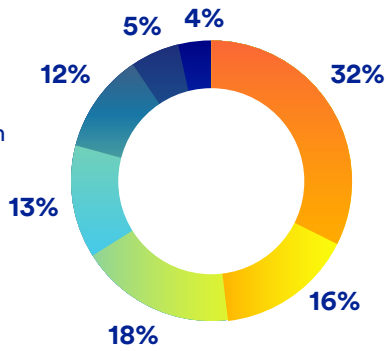


Age of respondent



Geographic regions

- North America: The USA and Canada
- South America
- Europe and United Kingdom
- Asia-Pacific
- Middle East and Africa
- North America: Mexico
- Central America and Caribbean

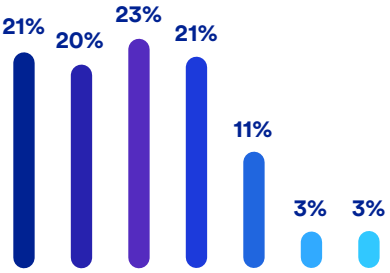


Organizational revenue (EUs) (US$)

$500,000-$4.9M	17%
$5M-$24.9M	10%
$25M-$199.9M	10%
$200M-$499.9M	8%
$500M-$999.9M	6%
$1B-10B	7%
$10B+	5%
Unable to disclose	38%

Global organization employee count (EUs)

- 1-20
- 21-200
- 201-1,000
- 1,001-10,000
- 10,001-100,000
- 100,001-500,000
- 500,000+

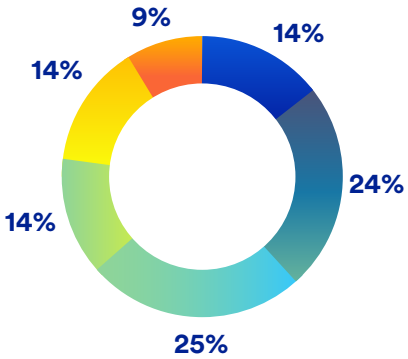


Physical security department employee count

1-20 employees	50%
21-200 employees	32%
201-1,000 employees	11%
1,001-10,000 employees	5%
10,000+ employees	2%

Video surveillance deployment (# of cameras) (EUs)

- 1-9
- 10-100
- 101-500
- 501-1,000
- 1,001-5,000
- 5,000+



Access control deployment (# of card badges or touchless access readers) (EUs)

20 cardholders	13%
21-50 cardholders	8%
51-100 cardholders	6%
101-500 cardholders	16%
501-1,000 cardholders	10%
1,001+ cardholders	35%
None of the above/NA	11%

Appendix 3 – 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: C02. What technology do you have deployed in the physical security environment at your organization? Other, please elaborate:

- Audio analytics
- Disaster recovery and emergency response technology
- Drones
- Gunshot detection
- Handheld thermal cameras
- Health and safety technology
- Key management system
- Magnetometers
- Panic buttons
- Situational awareness management system
- Threat management
- Under vehicle scanning system
- Weapon/explosive detection
- Weather system
- X-Ray screening

Channel partners: CA04. What kind of physical security technology does your organization most commonly install/deploy?

Other, please elaborate:

- Automatic gates and parking system, X-ray and metal detection gate
- Blast Design and HVM
- Cash in transit management
- Mail scanning, Gun-shot detection, Emergency Mass Notification
- Professional radio infrastructures
- Temperature control with thermal cameras

End users: C07. How is your organization's physical security infrastructure structured?

Other please specify:

- Local monitoring at TOC - Traffic Operations Center
- Local monitoring by surveillance team, some remote monitoring capability
- Local monitoring of all cameras by department
- Local police monitoring of surveillance
- Nobody is in charge, people who notice intrusion may investigate if they have time to
- Panic buttons
- Reactive with little to no monitoring
- We are exploring remote monitoring by 3rd party alarm monitoring company

End users H03. What kind of data are you collecting into your security operations center (SOC) from other systems?

Other, please elaborate:

- Casino game activities
- Crime related data is collected
- Localized crime data
- Parking management
- Patient information, laboratory results, imaging (Ultrasound, X-ray, CT scans, etc.)

- Travel Security - traveler information

Channel partners: CE07. Will other operations be affected by work on your deployment backlog?

- (Previous question mentioned the following operations: New system sales, Service renewal sales, Ability to keep up to date with industry innovation)
- Billing and collection
- Bug fixes
- Cybersecurity
- Delivery times
- New hiring
- Staff training (Sales and Technical)
- Testing and quality assurance: Deployment backlogs can have an impact on testing and quality assurance processes
- Cloud

End users: D09. Has anything else slowed your organization's adoption of cloud-based solutions for physical security applications?

- Clarity issue from the Government
- Cloud compliance issues in the org
- Installation of fiber by the service provider
- Lack of confidence in the continuity and quality of the services of Internet suppliers
- Network infrastructure ability to support cloud hosting
- No desire to move anything to cloud for physical security.
- Optimising our current security protocols with the cloud sometimes takes longer than expected to pair and stay updated
- Organization culture
- Our university is very reactive and tends to not make decisions until absolutely necessary.
- Prefer local security
- Redundancy in case of failure or loss of communication
- Senior leaderships lack of technical understanding therefore keeping a status quo
- We are actively working to leave the cloud and return to an on-premise solution

Channel partners: CC08. Has anything else slowed down the adoption of cloud-based solutions?

- Attitudes to OpEx cost models and perpetual cost.
- Benchmarks are not used to balance data between platforms
- Complex data retention policies (Data ownership and storage for Microsoft/Google/AWS, etc.), without hard commitments, Governments and high-risk objects will not yet move to cloud soon. Also Infrastructure conditions (e.g. Fiber) in local countries play a role
- Conservative minded public safety practitioners with a desire to keep control of their data
- Customer depending on the price variations of the host. Customer taken hostage on progressive raising pricing.
- Lack of cloud knowledge and education
- Most of our customers simply don't need the features it provides
- OpEX vs CapEX expenses; lack of clarity regarding internet outages
- Some organizations have a large number of traditional systems and applications, and integrating them into the cloud can be complex, which may slow down the adoption of cloud solutions.

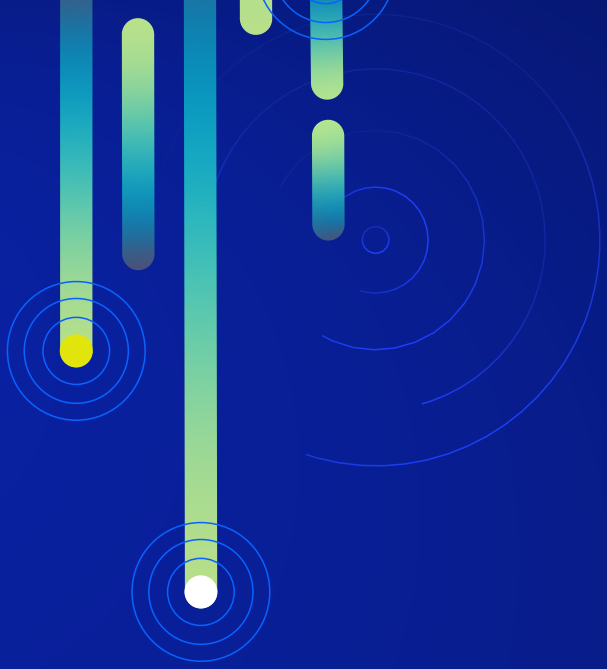
End users: D13. Has anything else led your organization to begin using the cloud for physical security applications?

- Because hackers manipulate systems we had few encounters with intrusions we failed to trace ...since we now have surveillance stored in the cloud it's easier to keep in saved and secured.
- Business Resilience Policy
- By utilizing cloud solutions, we can leverage the expertise of cloud service providers' professional teams to monitor and maintain our physical security applications, thereby alleviating the burden on our internal teams.
- Cloud platforms facilitate collaboration and information sharing, enabling security teams to collaborate more effectively in handling security incidents and threats.
- Cloud providers typically possess dedicated security teams, better equipped to address potential security risks, thereby reducing my risk exposure.
- Cloud solutions allow you to centrally manage physical security applications across multiple locations, whether these locations are in different cities or different countries.
- Convenient and easy to manage
- Cost savings by not deploying corporate network to some medium sized sites
- Eliminate physical servers
- In a cloud environment, you can achieve rapid disaster recovery, enabling swift restoration of normal operations even in cases of failures or data loss.
- The rest of the business is moving to the cloud
- There is faster storage in the cloud!
- Updating and scalability
- We can leverage the expertise of cloud service providers' professional teams to monitor and maintain our physical security applications, thereby alleviating the burden on our internal teams.

Channel partners: CC06. Are there other drivers causing end users to begin considering using the cloud?

- Additional capabilities which evolve with time
- AI support, Machine learning and speed of (new) technology developments in cloud
- Always remains operational. No intelligent hardware data that can be lost.
- Backup copies for ransomware
- Being able to review information from anywhere and not only physically as before.
- Better ROI and low CAPEX
- Buzzword compliance!
- Centralize information on an expert operator to quickly review any locality
- Centralized case and evidence management
- Cloud computing allows users to easily scale up or down their resources as needed. This is especially important for businesses facing rapid growth or fluctuating demand.
- Cloud is the general trend of Internet development
- Cloud providers offer AI and machine learning services that enable users to develop and deploy AI-driven applications without the need for extensive expertise in these fields
- Cloud security providers may offer tools and features that help organizations comply with industry-specific regulations and data protection requirements.

- Cloud security providers often have specialized expertise and resources dedicated to security, which can be beneficial for organizations that lack in-house security expertise.
- Cloud security solutions can help ensure the security of remote access.
- Cloud security solutions can provide robust business continuity and disaster recovery capabilities, ensuring the availability of data and systems.
- Cloud security solutions typically exhibit a high degree of scalability, allowing for rapid expansion or contraction as per requirements. This capability is particularly vital in addressing business fluctuations.
- Cloud technology hype
- Cloud-based security platforms often provide access to real-time threat intelligence and analysis, enabling organizations to stay ahead of emerging threats and vulnerabilities.
- Cloud-based security solutions can be accessed from anywhere with an internet connection, making them suitable for organizations with a global presence or remote workforces.
- Cloud-based security solutions can offer robust disaster recovery capabilities, ensuring that data and systems do not depend on physical hard drives that can be stolen
- Don't want to maintain servers
- Greener
- In the long term you only pay for what you use and need
- Innovation and time-to-market: Cloud computing provides a platform for rapidly developing and deploying new applications and services. It allows organizations to experiment, innovate, and bring products to market faster.
- IOT and hardware device not fully compatible with cloud
- Many organizations are adopting a cloud-first strategy for various aspects of their operations. Integrating security with other cloud services can streamline operations and enhance overall security.
- Migration from a complete office environment to the cloud, recommendation systems must then come along. No more servers locally.
- OPEX model preferred
- The theft or manipulation of the CCTV recorder, allowing to have the backup in the cloud and not local



About Genetec

Genetec Inc. is an innovative technology company with a broad portfolio of physical security solutions. The company's flagship product, Security Center, is an open-architecture platform that unifies IP-based video surveillance, access control, automatic license plate recognition (ALPR), communications, and analytics. Genetec also develops cloud-based solutions and services designed to improve security, and contribute new levels of operational intelligence for governments, enterprises, transport, and the communities in which we live. Founded in 1997, and headquartered in Montreal, QC, Canada, Genetec serves its global customers via an extensive network of resellers, integrators, certified 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