December 2022

State of Physical Security 2022:

Effectively navigating a changing landscape

Research insights from over 3,700 physical security professionals

STATE OF PHYSICAL SECURITY
3RD
ANNUAL
2022

Genetec™

Contents

About the research

Genetec Inc. surveyed physical security professionals from August 24 to September 21, 2022. Following data cleansing and a review of submissions, 3,711 responses were included in the sample for analysis.

Some details about the survey methodology

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

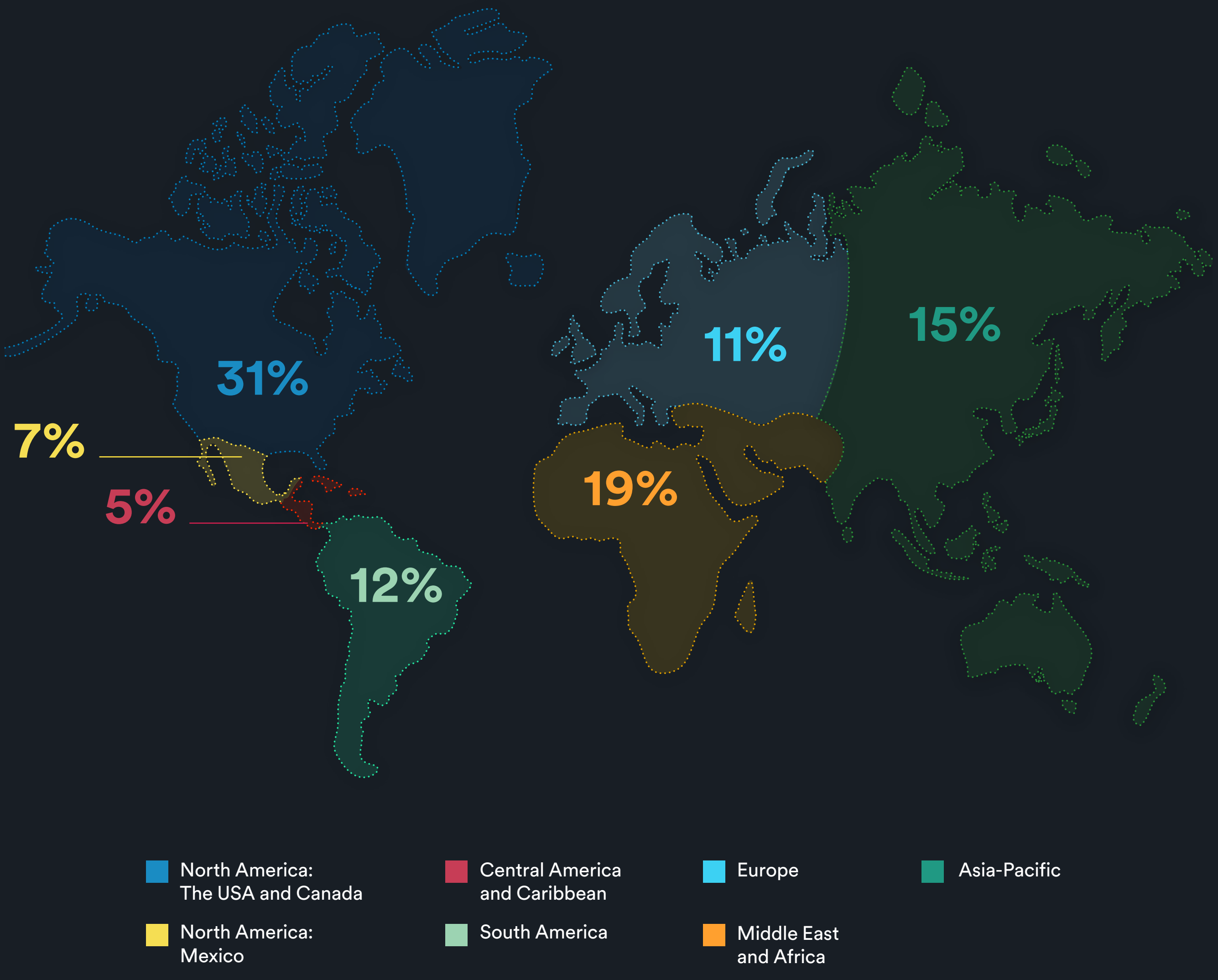
- **End users** (individuals working for organizations participating in the procurement, management, and/or use of physical security technology) and
- **Systems integrators, installers, and providers** (individuals who consult on, integrate, install, sell, or service security solutions)

The target population was reached by third parties via their opt-in email lists, Genetec opt-in email lists, and digital promotions. Some of the results in this report are based on responses from both end users and systems integrators/installers/providers. However, some questions were only asked to end users and some only to systems integrators/installers/providers. This report points out whether answers are from all respondents, end user respondents, or systems integrators/installers/providers respondents.

Even for the questions asked to both groups (end users and systems integrators/installers/providers), each result was analyzed by responses from ‘end users only’ and ‘systems integrators/installers/providers only’, as well as by both groups combined. In most cases, there was little difference in the results. Responses from ‘end users only’ were in line with responses from ‘systems integrators/installers/providers only’. The report points out instances where this wasn’t the case. It also highlights instances where the percentage of responses differs significantly by geographic region, end user industry, or by organization size, measured by the number of global employees.

BACK TO TABLE OF CONTENTS

The target population was sampled across all geographic regions.



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.

BACK TO TABLE OF CONTENTS

Executive summary

Organizations are taking stock and settling into a new way of working after a period of uncertainty and change driven by the COVID-19 pandemic. Many of the results from the 2022 survey were similar to the responses from the 2021 survey. But some also uncovered new challenges faced by the industry, like product shortages and human resource issues.

What's clear is that organizations are ready and able to adapt, and are looking to the future when it comes to the application of physical security technology:

The future of cloud is hybrid: Many organizations envision a blend of on-premises and cloud-based solutions for their physical security deployments as they look to optimize their infrastructure investments and leverage hybrid options to save costs and increase efficiency.

The influence of cybersecurity and IT: Cyber concerns are on the rise and are inspiring new methods to implement and maintain a strong cybersecurity strategy.

The use of physical security for business operations: The pandemic pushed more organizations to leverage multiple systems and data sources to better manage their facilities and flow of people. The trend to consider physical security solutions as more than just a cost associated with protecting people and assets will continue, and new approaches to how physical security data is used will inform organizational and operational decisions.

Overcoming supply shortages: The industry adapted to supply chain issues by extending the value of their existing hardware or delaying projects. With 2023 budgets remaining healthy, security and IT departments are planning to complete deployments or start new projects as components become readily available.

Summary of differences around the world

For most questions in our survey, there were slight differences between regional respondents. In other words, the percentage of responses for each answer and each region was similar. This suggests a consistent global view of how physical security has developed over the last year.

Below are the instances in which answers from a specific region differed significantly from the global average.

Asia-Pacific: Supply chain and cloud

Systems integrators from Asia-Pacific are more pessimistic about the impact of supply chain issues in the next year. 57.5% answered that the supply chain problems would either "greatly increase" or "somewhat increase". This is above of the global average of 49%.

Respondents were asked to apply a ranking to the different reasons for slowly adopting the cloud. Overall, "perceived cybersecurity risks" has the highest average ranking. In Asia-Pacific, the highest is "fear of data loss" closely followed by "lack of understanding of the cloud".

The Asia-Pacific region is ahead in private cloud use. Most respondents globally still store their video in on-premise storage devices (e.g. NVRs, servers, NAS, SAN). In Asia-Pacific 4.55% selected they stored their video data "mainly in a private cloud", the highest of any region.

Central America and the Caribbean: Unification and cloud

Unified security systems are less common in Central America and the Caribbean. "My organization's video surveillance and access control systems are not connected (they are separate systems)" was the second most common answer selected. In all other regions, this was the least common answer.

Respondents from Central America and the Caribbean also indicated they use public cloud storage more frequently than in other regions. 6.9% of Central American and Caribbean respondents selected "Mainly stored with public cloud storage services" compared to 2.6% globally.

BACK TO TABLE OF CONTENTS

Europe, Middle East, Turkey and Africa: Cloud, credential threat, and supply chain

EMEA is the most conservative region when it comes to cloud adoption within physical security. 69% of respondents stated that they have not moved any of their infrastructure to the cloud compared to a 58% average globally.

EMEA respondents confirmed that "credential theft" is the greatest threat to their organizations with 50.2% selecting this option versus 39.6% globally.

Europe experienced the most challenges with project delivery in the last 12 months with 82% of respondents stating that they were impacted, compared to 71% globally. This can be attributed to budget reductions and supply chain issues. Despite these challenges, respondents stated that most projects were not canceled but delayed into 2023.

Mexico: Cloud

Only 17.4% of respondents from Mexico suggested that COVID-19 somewhat accelerated their cloud strategy. This compares with 30.9% globally. They also had the lowest portion of respondents (29.4%) indicating that it was "somewhat" or "greatly" accelerated, compared with 46.7% globally and 47.9% in the USA and Canada combined.

Mexico also selected that COVID-19 had "triggered" their cloud strategy more commonly than any other region (9.8%). A stark contrast with the USA and Canada where only 0.35% of respondents selected this (by far the lowest of any region).

South America: Remote work and cybersecurity

50.4% of respondents from South America said their organizations have no physical security staff set up to work remotely, while the global average is 33.7%.

They were also the least likely to have identified "better cybersecurity strategy" as one of the new processes they prioritized this year. Only 38% of respondents selected this compared with 49.2% globally and 52.9% in the USA and Canada.

The USA and Canada: Fewer layoffs, temperature reading, and unification

41% of the USA and Canadian respondents indicated that "none" of their security employees had been laid off in 2021. This compares with 29% globally.

Temperature reading technology was less frequently selected by the USA and Canadian respondents than by all other regions, 14% versus 24% globally.

Unifying video and access control systems were second most common in the USA and Canada with 80% of respondents indicating that their systems were unified compared with 77% globally.

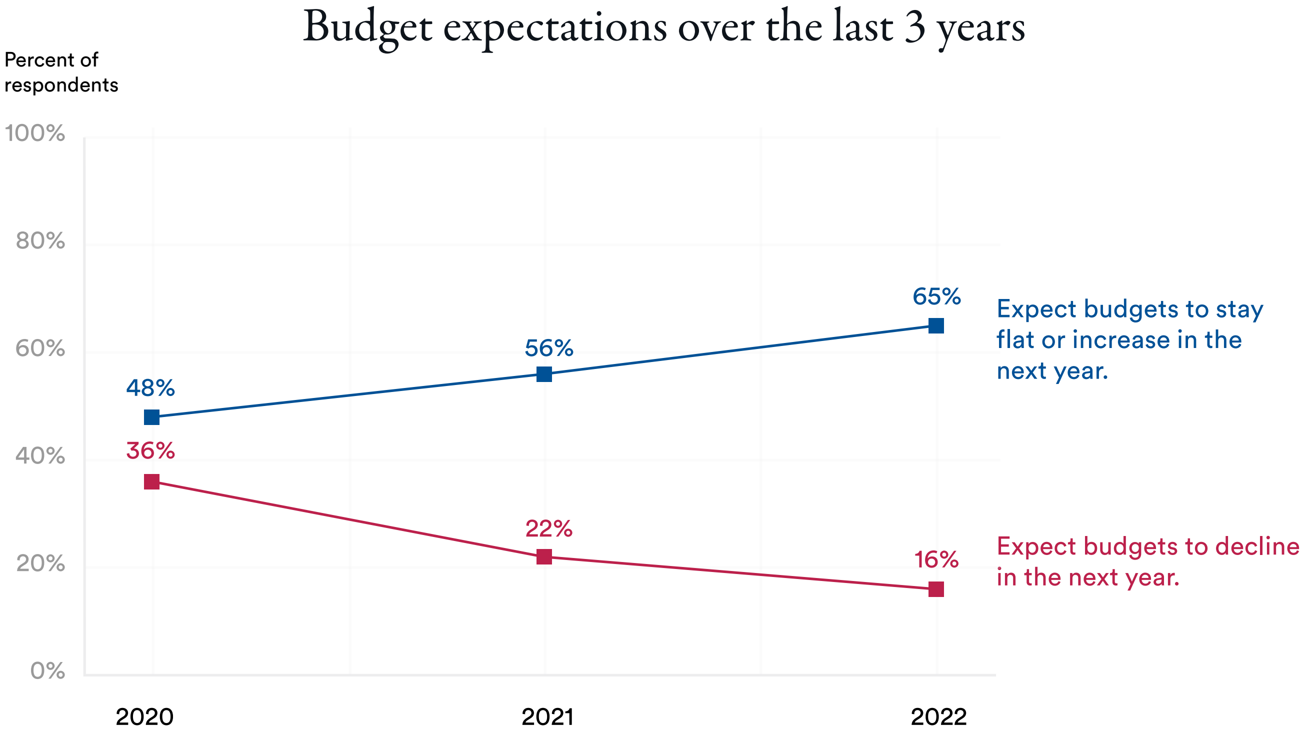
BACK TO TABLE OF CONTENTS

Key findings

OPEX budgets grow

With a challenging economic outlook for 2023 that is predicting a recession in many countries, it's important to note that in previous downturns and recessionary periods, the physical security market continued to grow. This resilience seems to be reflected in survey results with the overall outlook for OPEX budgets remaining positive for 2023 and continuing to rebound from the results of the pandemic:

OPEX BUDGETS



Given the different economic conditions worldwide, responses to this question did not vary significantly by region. This reflects an overall optimistic view across the physical security industry.

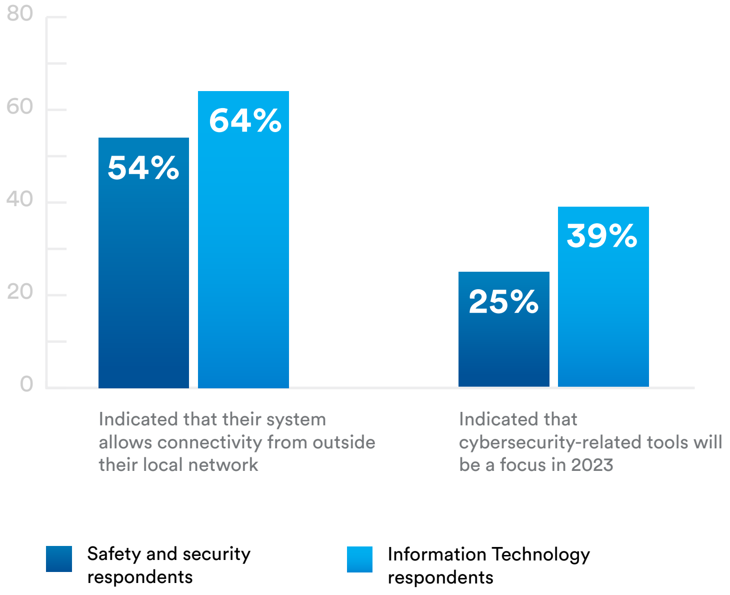
BACK TO TABLE OF CONTENTS

IT plays a larger role in physical security

A decade ago, most physical security systems in larger organizations were managed by personnel in specialized security departments. However, 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 network and technology governance. It’s no surprise that in our 2022 survey, respondents who identified their job function as “Information Technology” had a different point of view than their counterparts who selected “Security and Safety”. Network and cybersecurity issues were prioritized in the responses of “Information Technology” respondents related to the management and deployment of these physical security systems.

IT VERSUS SECURITY

Prioritizing cybersecurity tools



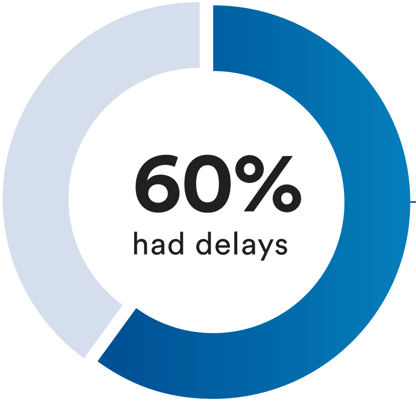
IT respondents see ransomware, engineering/phishing, and remote execution attacks as a greater threat to their organization than Safety and Security respondents.

BACK TO TABLE OF CONTENTS

Competing for components

In 2021, there were rules and restrictions due to the pandemic, as well as challenges in Taiwan factories, blockages in the Suez Canal, and difficulties in ports of entry. Combined with a massive increase in component demand across industries (such as smartphone and car manufacturers) and the new "at home" needs of consumers, this led to unprecedented shortages of physical security hardware and delays to projects.

Results of the survey demonstrate the widespread effects of supply chain problems and how physical security practitioners worked pragmatically to manage them.



60% of end users indicated that physical security projects had been delayed due to supply chain issues. Many of the delays were for long periods.

- 46% of end users faced more than 3 months of delays.
- 28% of end users faced more than 6 months of delays.

Many different types of projects were delayed. For end user respondents that faced delays, the replacement of technology or equipment was the most difficult (66%) followed by the expansion of current installations (51%) and upgrades (51%).

For suppliers of video surveillance hardware, delays had serious implications as 45% of end users looked for alternatives and changed brands to deploy available equipment.

Systems integrators also outlined the need to try different strategies to cope with hardware shortages including the use of "second-hand equipment" and "a repair center to bring back some easy-to-fix electronics into production".

Viewpoint

The COVID-19 crisis and subsequent impact on hardware and electronic components availability have highlighted the critical role supply chain and logistics play in most industries.

While the pandemic is mostly behind us, the new socio-economic situation and uncertainty triggered by the current geopolitical conflicts are continuing to put a strain on the global supply chain.

For the security industry, that translates into systems integrators needing to:

- Continue placing hardware orders well in advance of projects to secure their material when needed
- Develop closer relationships with partners who can provide potential alternatives to back-ordered products
- Associate with vendors that are resilient and adaptable, and that can quickly re-engineer their products based on raw material and component availability

On a positive note, early indicators point to the supply chain bottlenecks easing in 2023, which should provide much-needed relief for systems integrators looking to deploy new projects in a timely fashion.

Nadia Boujenoui
Vice-President of Customer Experience
Genetec Inc.

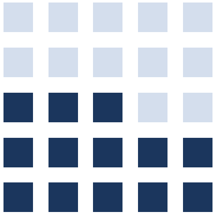
BACK TO TABLE OF CONTENTS

Human resources face many challenges

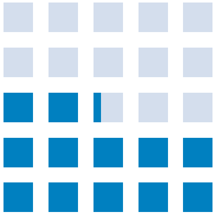
Across all industries talent shortages, back-to-the-office plans, and employee expectations for new ways of work challenged organizations over the last couple of years. The results of the survey demonstrated that the physical security industry was no different.

50% of all 2022 survey respondents indicated that their physical security organization had experienced HR challenges in the last year. Respondents commented that challenges resulted in the need to shift and reassign staff, and that time and budget for training were limited.

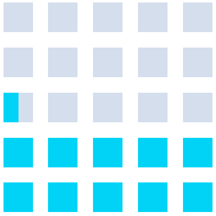
For respondents that faced such challenges:



52%
Faced staff shortages



49%
Faced hiring difficulties



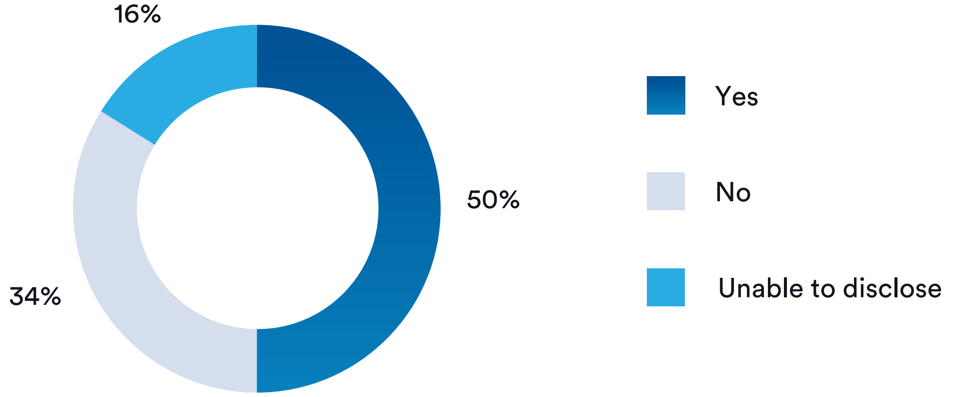
42%
Faced employee morale problems

The survey revealed that out of the 48% that prioritized the above, 83% are from the cannabis sector and 73% are from the gaming sector.

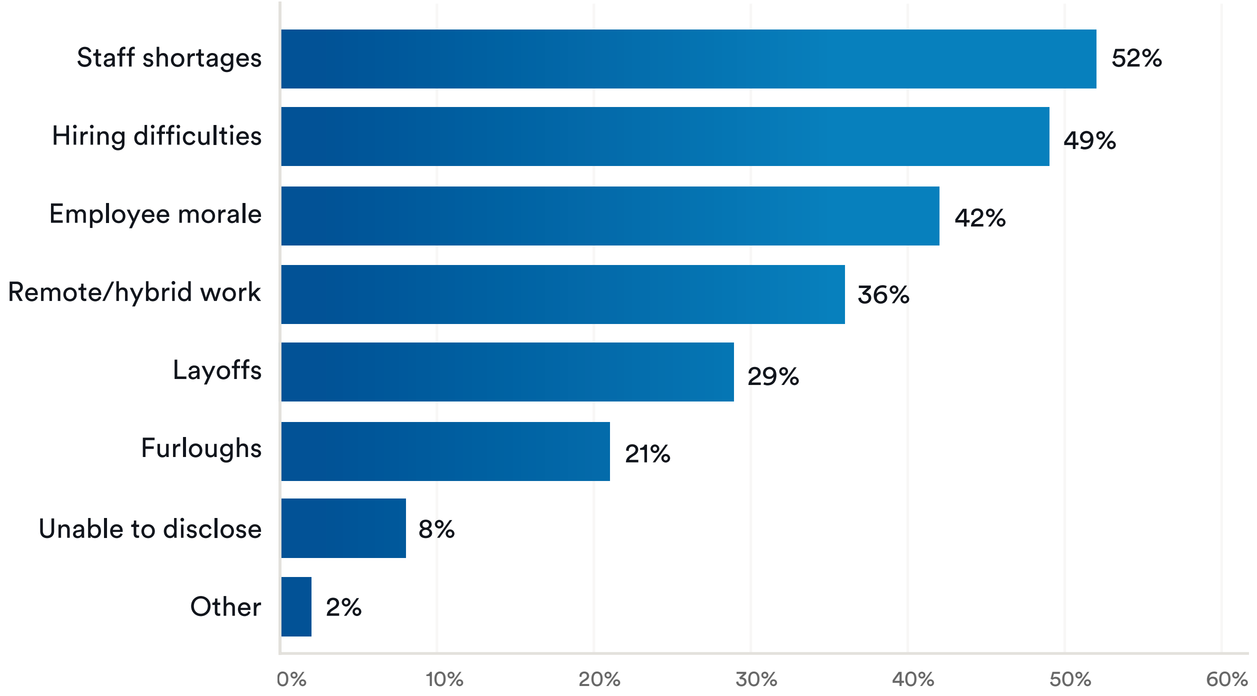
BACK TO TABLE OF CONTENTS

HUMAN RESOURCES FACE MANY CHALLENGES

Has your physical security organization experienced HR challenges in the last year?



What kind of HR challenges affected your physical security department in the last year?



BACK TO TABLE OF CONTENTS

Observations on cloud adoption

Cloud acceptance by region

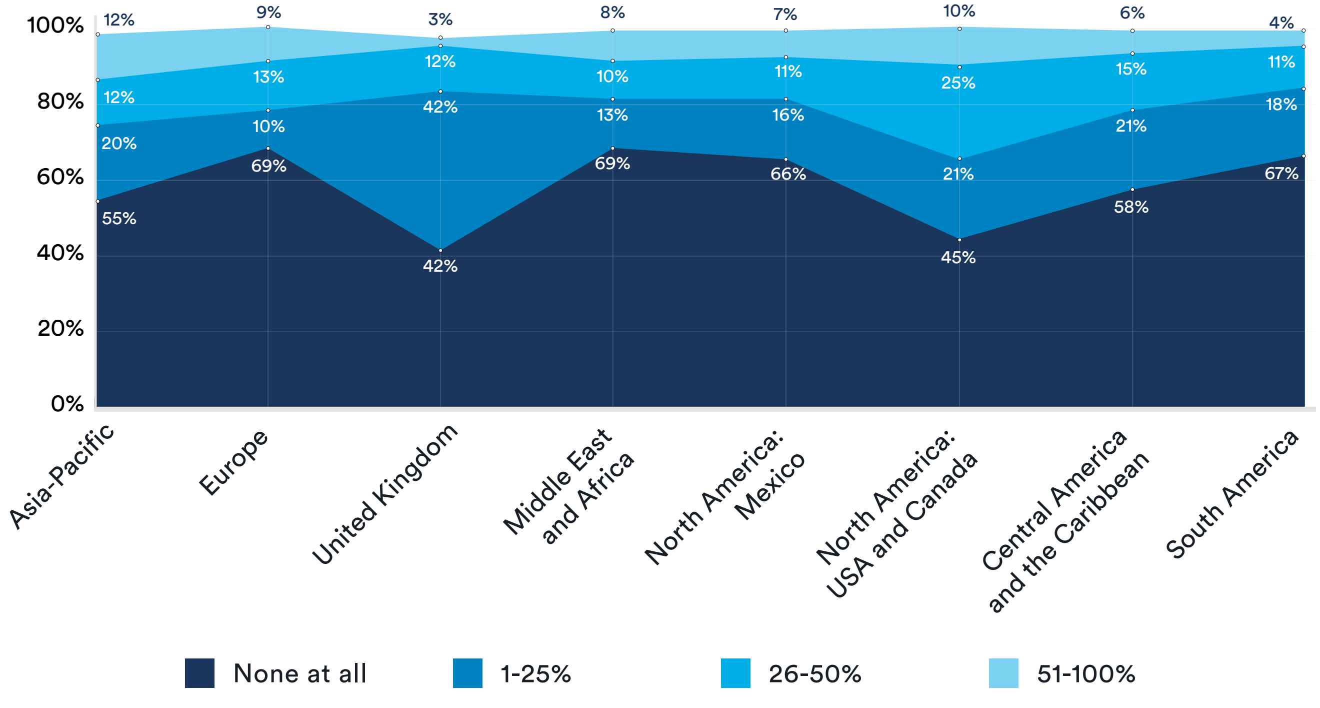
Most end user respondents (82%) indicated that they mainly store video footage in on-premise storage devices (e.g. NVRs, servers, NAS, SAN). Just 6% indicated that they use either public or private cloud for this purpose. The top driver is to leverage remote work, which makes sense as fewer people are going into the office on a regular basis.

The percentage was highest in the retail end user sector, where 81% of respondents indicated that they would make the move to the cloud. Also, a lower percentage of respondents in Europe and the Middle East thought their organization would move to managing or storing their physical security data in the cloud than in other regions.

Almost 2/3 of all respondents indicated that, during the next two years, their organization will move to managing or storing more of their physical security data in the cloud.

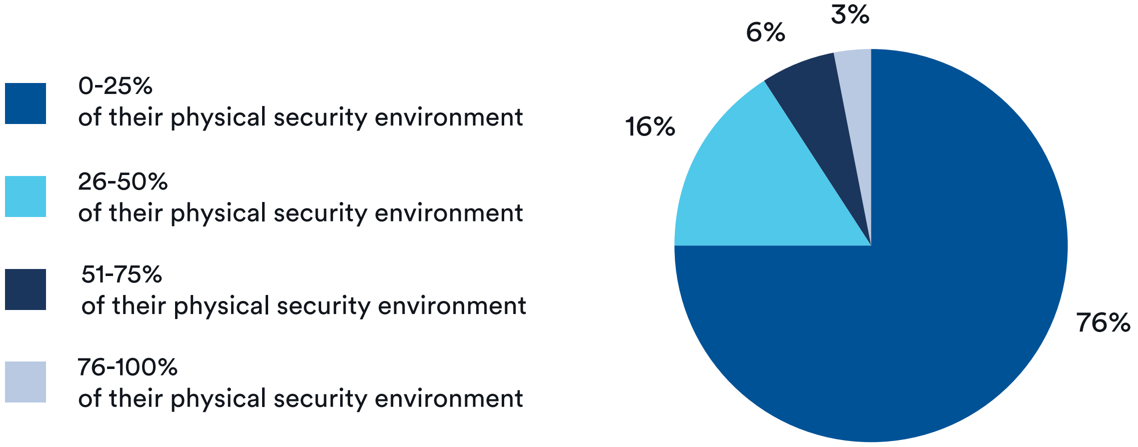
OBSERVATIONS ON CLOUD ADOPTION

Cloud or hybrid-cloud adoption by region



BACK TO TABLE OF CONTENTS

How much of your physical security environment is cloud or hybrid-cloud? (Select one)

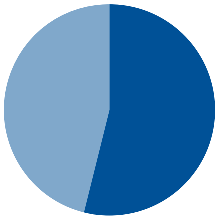


This movement to the cloud is consistent with forecasts from industry analysts. Novaira Insights reported that in the Americas the percentage of video management software revenues that come from cloud video management software will grow from 19% in 2021 to 45% in 2026.

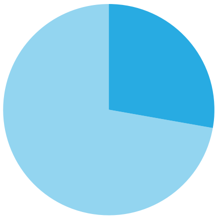
BACK TO TABLE OF CONTENTS

OBSERVATIONS ON CLOUD ADOPTION

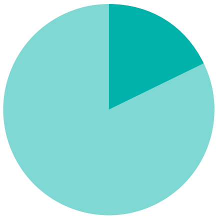
The future looks hybrid



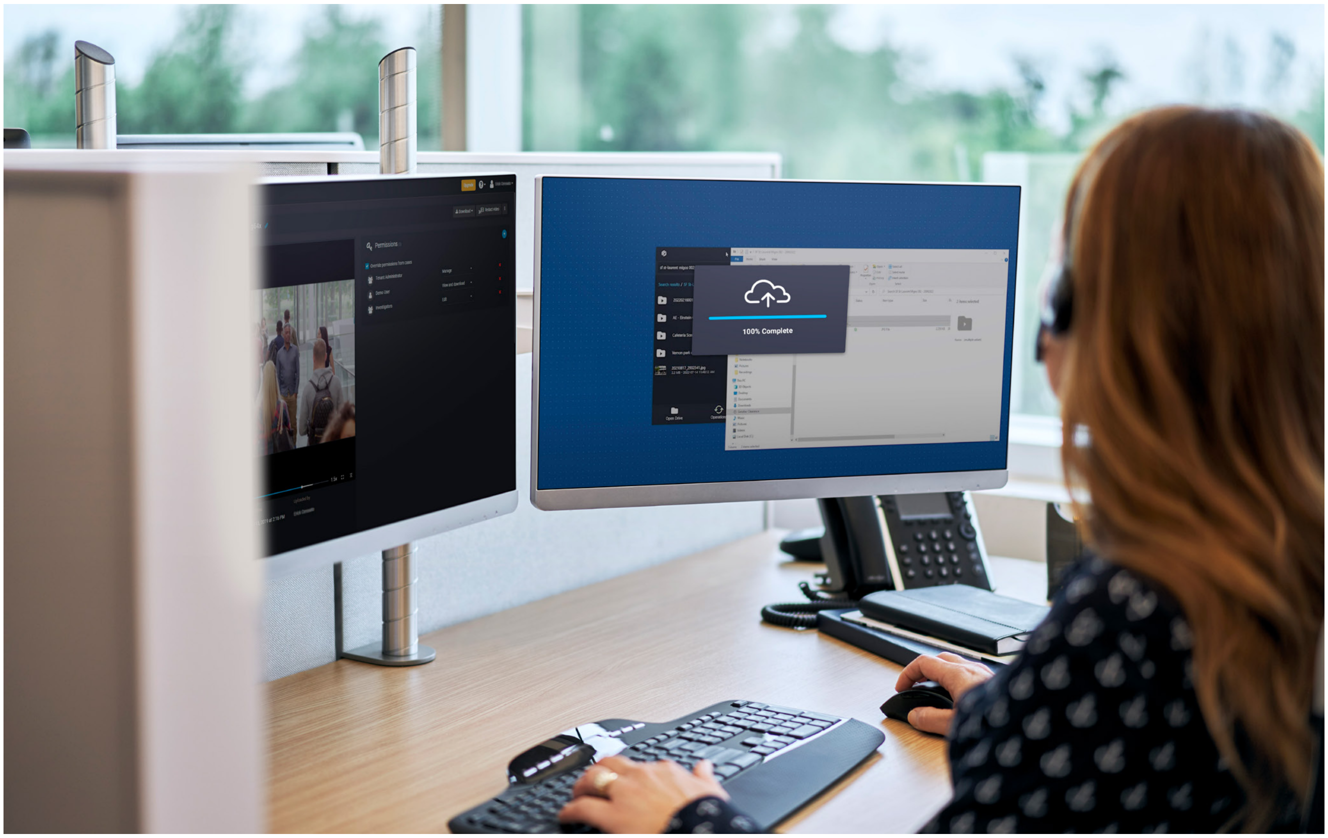
54%
of end users indicated moving toward a blend of on-prem and cloud-based solutions



28%
of end users indicated all cloud-based solutions

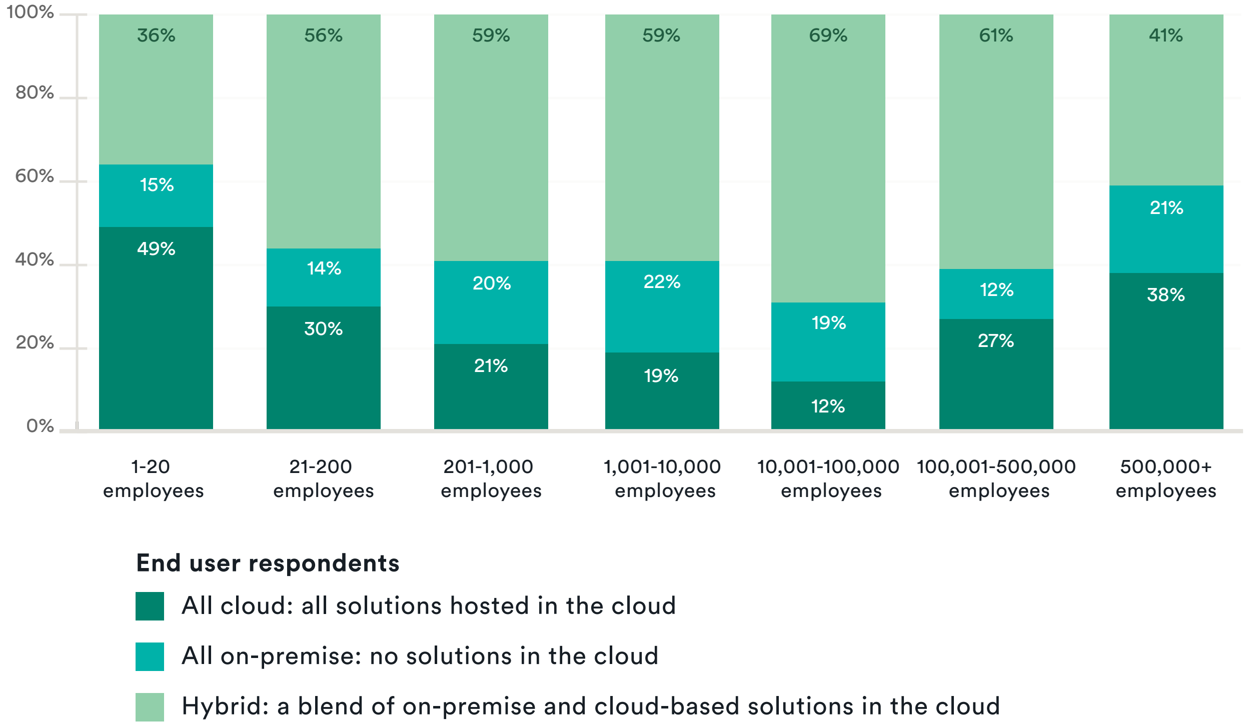


18%
of end users indicated no cloud-based solutions



BACK TO TABLE OF CONTENTS

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



Cybersecurity is a barrier

The physical security industry is still lagging behind other industries in its adoption of the cloud. Perception of the technology among security professionals remains conservative. The perceived cybersecurity risks of the cloud were ranked as the most prominent reason for slowing cloud adoption. This could be viewed as a somewhat self-fulfilling barrier and one based on a lack of understanding of the inherent cybersecurity of cloud-based solutions.

In the healthcare sector, 26% of end user respondents indicated that no solutions would be hosted in the cloud, and in the state/local government sector this was 24%. While these sectors may be warming up to placing their office productivity tools in the cloud, there seems to be residual resistance to moving their physical security workloads there.

> "Lack of culture for using [cloud] technology [in physical security]"
>
> – End user survey respondent

BACK TO TABLE OF CONTENTS

Viewpoint

Cybersecurity doesn’t have to be a barrier to cloud adoption. You need to have the controls, partners, procedures, and mechanisms in place to manage risk. It’s about a shared responsibility model which can be highly secure if you make the right choices and cooperate with the right partners.

Mathieu Chevalier
Genetec Manager and
Principal Security Architect
Genetec Inc.

BACK TO TABLE OF CONTENTS

Physical security and related data are mission-critical

During pandemic restrictions, physical security was often used to aid with the safe movement of people around buildings. It could help with such things as maintaining social distancing, people counting, and verifying that occupants were wearing masks. However, now that pandemic restrictions have largely ended, physical security is still viewed as more than a tool to respond to crime or a necessary expense to keep assets and people safe. It has become a core element in the digital transformation of organizational processes.

63%

of end user respondents indicated that physical security and related data were mission-critical. This was similar to the 2021 survey (68%).

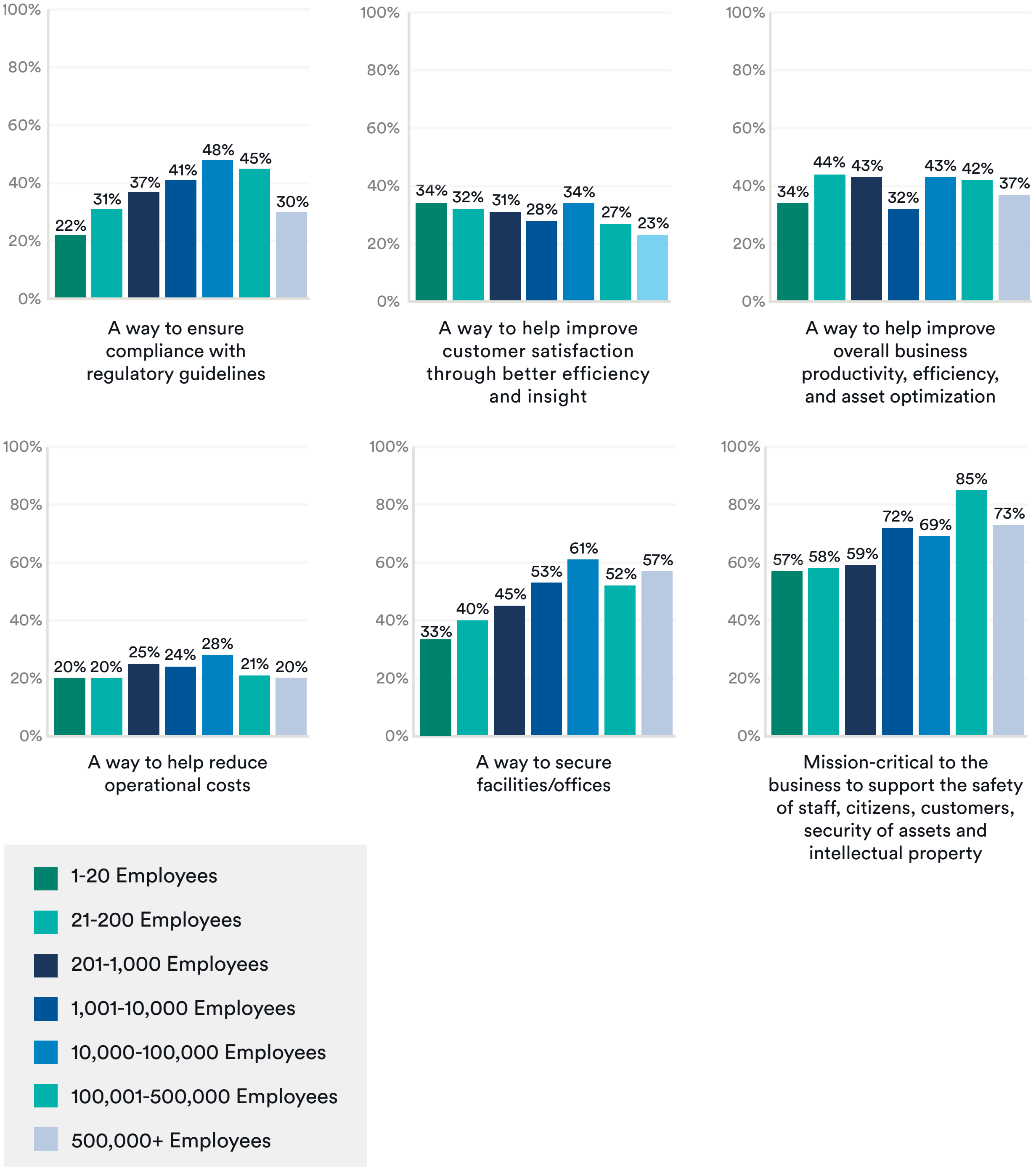
In particular, video surveillance offers a rich source of data. Organizations may already have sufficient video surveillance systems installed but can utilize existing data to fundamentally change business processes via the creation of new outputs and/or additional value. Examples include monitoring customer queue lengths in retail organizations or decreasing traffic congestion levels in city centers by timing traffic light signals.

It also appears that as organizations grow, their views on the value and/or use of physical security data change. A higher percentage of end user respondents in organizations with over 100,000 employees indicated that physical security and related data were mission-critical than in organizations with fewer employees. This may be because they are further along in their digital transformation initiatives than smaller companies. Having sufficient data management and structure is key to unlocking additional value from data gathered across physical security systems.

From an end user sector perspective, a notable outlier with the highest percentage of respondents indicating that physical security and related data were mission-critical was the transportation end user sector (71%). Here, physical security plays not only a critical role in the safety of staff and passengers but helps meet strict standards for transit punctuality.

MISSION-CRITICAL ROLE OF PHYSICAL SECURITY

How organizations view physical security and related data by organization size



A way to ensure compliance with regulatory guidelines

A way to help improve customer satisfaction through better efficiency and insight

A way to help improve overall business productivity, efficiency, and asset optimization

A way to help reduce operational costs

A way to secure facilities/offices

Mission-critical to the business to support the safety of staff, citizens, customers, security of assets and intellectual property

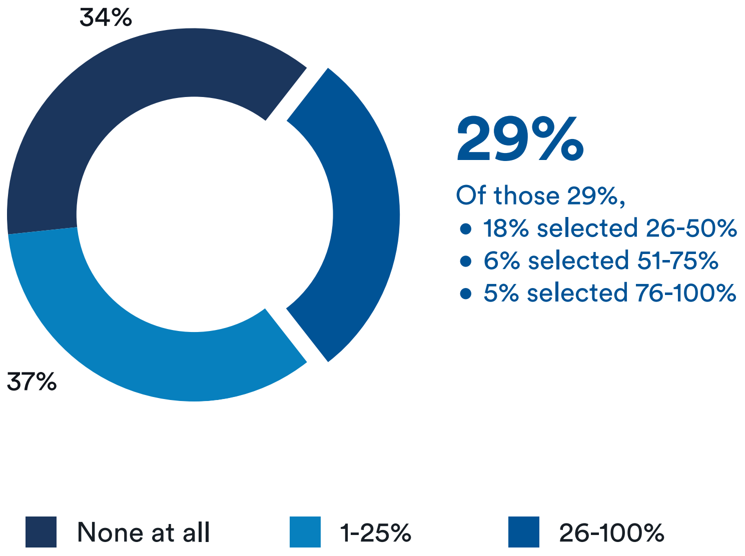
BACK TO TABLE OF CONTENTS

Cybersecurity is still the top priority

In the 2021 survey, 54% of respondents had more than 25% of their physical security operations staff set up to work remotely. In the 2022 survey, this fell to 29%.

CYBERSECURITY IS STILL THE TOP PRIORITY

What percentage of your organization's physical security operations staff are set up to work remotely?



29%

Of those 29%,
- 18% selected 26-50%
- 6% selected 51-75%
- 5% selected 76-100%

Interestingly, 46% of respondents in Europe and 48% in Latin America indicated that none of their physical security operations staff were set up to work remotely. This is compared with 21% in the USA and Canada and just 15% in the United Kingdom.

As pandemic restrictions have eased, remote work has declined. Despite this, as was the case in the 2021 survey, the top challenge faced by all respondents when managing employee and visitor safety remained cybersecurity. It's not surprising that 49% of all respondents indicated an improved cybersecurity strategy had been activated by their organization this year.

A higher percentage of all respondents in organizations with over 100,000 employees indicated that the top challenge they faced when managing employee and visitor safety was cybersecurity than in organizations with fewer employees. This could be due to the increased complexity of IT systems in larger organizations (including the number of devices to protect and manage) and the perception that this can increase cybersecurity vulnerability. It could also be due to the perception that larger organizations are more attractive targets for cybercriminals.

BACK TO TABLE OF CONTENTS

CYBERSECURITY IS STILL THE TOP PRIORITY

Where cybersecurity efforts are being focused

40%	access control
39%	cyber-hardening of security hardware
37%	strong password policies

The cloud perceived as a cybersecurity risk remains a major barrier to greater adoption of the cloud for physical security solutions. Respondents ranked such perceived risks as the most important factor in slowing the adoption of cloud-based solutions for physical security applications. Similarly, end users ranked such perceived risks as the most important factor in deterring their organization from deploying security systems to the cloud. Despite this, as shown earlier in this report, the gradual transition to the cloud for physical security continues.

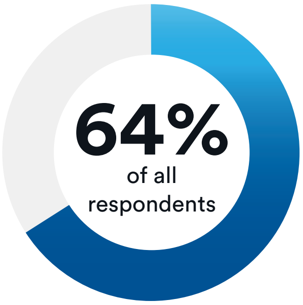
BACK TO TABLE OF CONTENTS

Physical security gets unified

For some, restrictions from the pandemic acted as a further catalyst to unify their video surveillance and access control systems as some end users needed to take this step to effectively manage the safe movement of occupants around their facilities. The increased demand for this approach may have caused some systems integrators to gain greater expertise and awareness of the benefits of unification, resulting in more recommendations to end users to consider this approach.

According to the survey responses, regionally, the USA and Canadian end users were the most likely to have deployed a unified video and access control system (where video and access control software are unified as one system from a single manufacturer).

> 44.4% of the USA and Canadian respondents selected they had deployed a unified video and access control system, higher than in all other regions.



have both video surveillance and access control in their physical security deployments.

⬇

Of those 64%, over 75% have either:

- Integration between video surveillance and access control systems from different vendors, or
- Unification of video surveillance and access control solutions from one manufacturer

Changes in technology – the past year

In the initial phase of the pandemic, interest grew quickly for a variety of security solutions that could assist with visitor management, implement government mandates, and improve remote capabilities. Interest in some of these solutions declined in 2021 and the latest survey suggests this has fallen further in 2022.

A lower percentage of all respondents in the 2022 survey indicated that capabilities associated with the pandemic were a priority. The 2022 survey also indicated that "traditional security-related" capabilities were the focus.

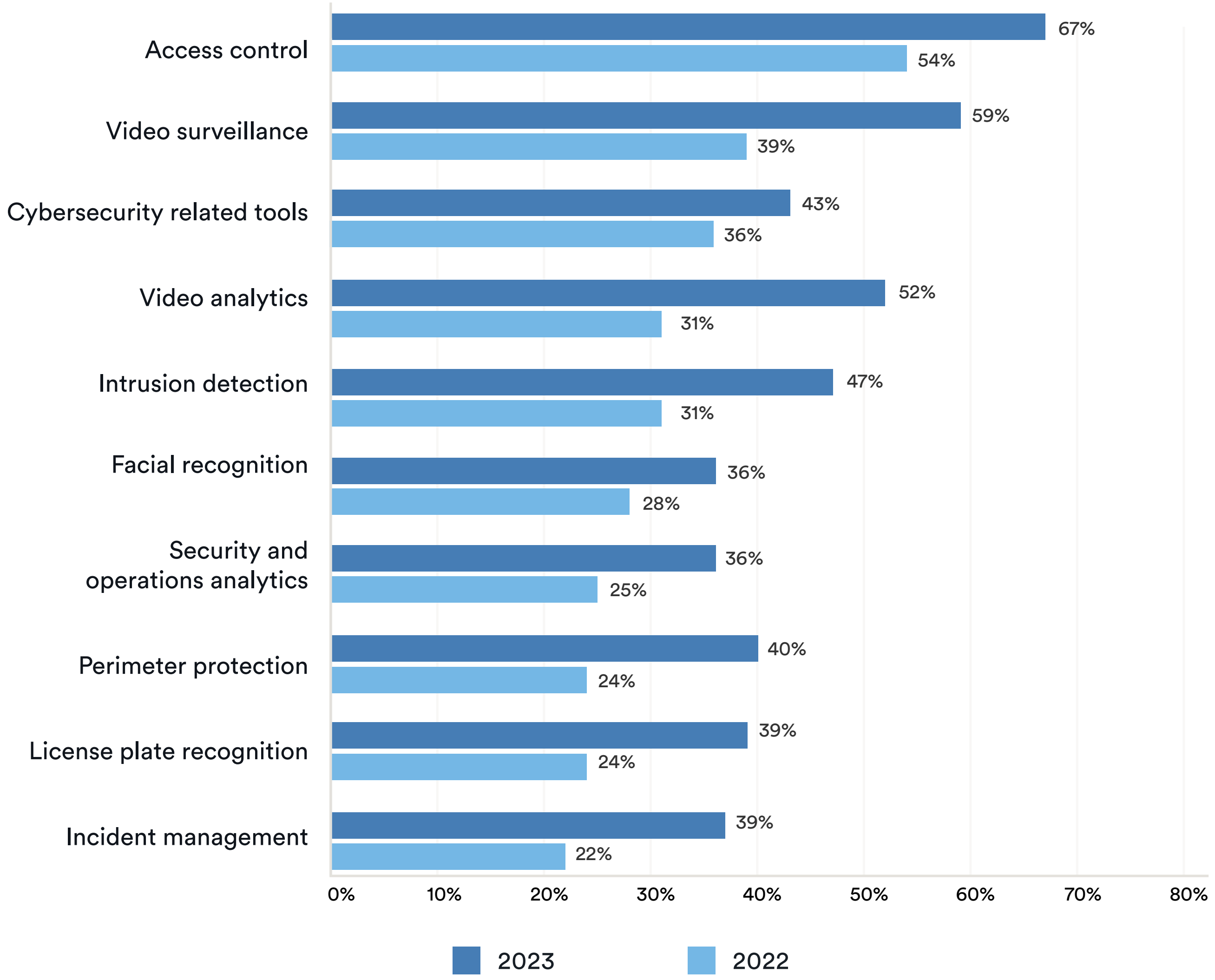
Changes in technology – the year ahead

As mentioned earlier in this report, the unification between access control and video surveillance has increased in importance for many organizations. Work that was set aside on core systems during the pandemic is now being reprioritized. Access control and video surveillance are two systems among others that are driving the focus on core system work into 2023.

BACK TO TABLE OF CONTENTS

CHANGES IN TECHNOLOGY - THE PAST YEAR VERSUS THE YEAR AHEAD

Top 10 technologies organizations are planning to invest in



BACK TO TABLE OF CONTENTS

Key takeaways

1 Economy and supply chain are challenges that can be overcome

Pandemic restrictions gradually began lifting in most countries in 2021 and 2022 but left behind real after-effects. These economic effects are impacting the physical security industry in the form of product shortages and HR difficulties. These factors were also present in 2022, and forecasts going into 2023 are uncertain making this an ongoing concern for businesses. Despite the effects of ongoing issues with the supply change, economy, and predictions of a recession, the survey points to an encouraging sign of an overall positive outlook for 2023 OPEX budgets.

2 Prioritizing the security of physical security systems

Although the physical security industry is behind in its focus on cybersecurity compared to other industries, it's evident that a shift has occurred and that the need to prioritize these initiatives as part of physical security system management has taken place. The top challenge faced in managing employee and visitor safety remained cybersecurity in 2022. This is also a top priority moving into 2023.

3 Move to the cloud continues

Although the physical security industry is still lagging behind other industries in its adoption of the cloud, there are clear signs that the move in this direction will continue. All things point to hybrid-cloud deployments being the way forward for enterprises so they can rationalize their costs, concerns, and approach to migrating to the cloud.

31%

of all respondents reported that budgets were expected to increase in 2023

34%

of all respondents reported that budgets were expected to remain flat in 2023

16%

of all respondents reported that budgets were expected to decline in 2023

36%

of respondents are looking to invest in cybersecurity-related tools to improve their physical security environment in the next 12 months

66%

of all respondents indicated that, during the next two years, their organization will move to managing or storing more of their physical security data in the cloud

BACK TO TABLE OF CONTENTS

Viewpoint

Shared services providers within end users are finding that they need to hone new skills to contend with:

- Growing involvement of other business stakeholders who have an interest in the underlying data
- Overcoming concerns around cybersecurity and the responsible use of the network
- Balancing an interest in leveraging technology advancements with internal constraints such as funding and talent shortages

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

Appendix

Appendix 1 - Survey methodology

Genetec Inc. surveyed physical security professionals from August 24 to September 21, 2022.

The goal of the research was to:

- get a view into physical security operations and environments
- understand organizations' response to external challenges such as product shortages and HR difficulties
- understand the global focus for 2023

Following a review of submissions and data cleansing, 3,711 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 study 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, 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 systems integrators. 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 by systems integrators).

A note about survey calculations:

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

BACK TO TABLE OF CONTENTS

Appendix 2 - Survey demographic information

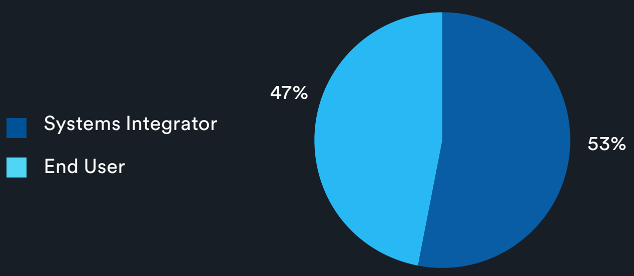
INDUSTRIES

Security Systems Services	55%
Others	8%
Education	6%
Transportation	5%
Banking and Finance	3%
Energy and Utilities	3%
National Security	2%
Engineering and Construction	2%
Manufacturing and Wholesale	2%
Technology and Media	2%
Healthcare	2%
Retail	2%
Public Administration	2%
Food, Cosmetics, Chemicals and Pharmaceuticals	2%
Transportation and Logistics	1%
Property Management	1%
Professional Services and Associations	1%
Gaming	1%

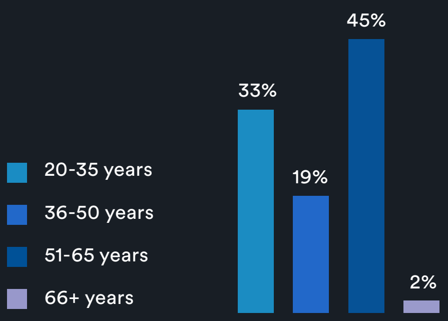
JOB FUNCTION

Engineering, R&D, System Design and Quality Assurance	23%
Facilities/Operations Management	14%
Sales	11%
Information Technology (IT)	10%
Customer Service or Support (incl. Technical Support)	8%
Project Management/Risk or Compliance Management	8%
Administration/Office Administration	6%
Security and Safety	5%
Accounting/Finance	3%
Administration, Legal	3%
Estimator	2%
Marketing	2%
Legal	1%
Purchasing and Procurement	1%
Quality Management	1%

RESPONDENT TYPE

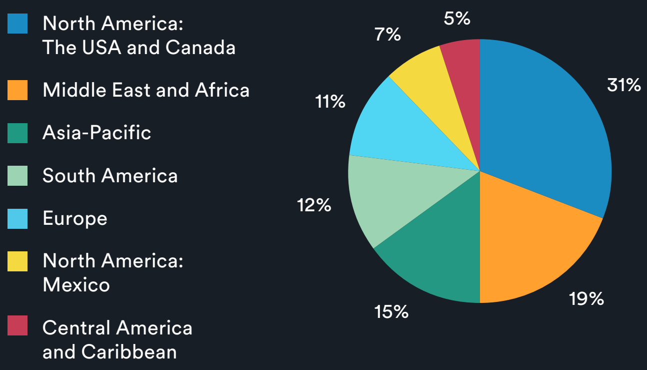


AGE OF RESPONDENT



BACK TO TABLE OF CONTENTS

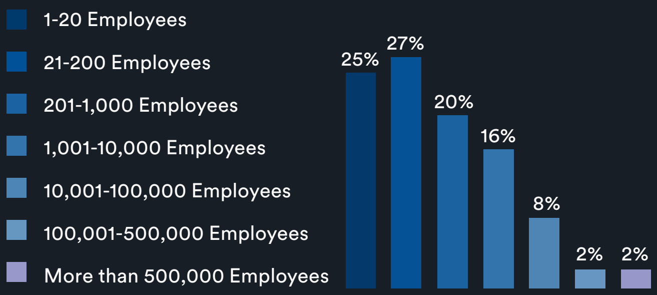
GEOGRAPHIC REGIONS



ORGANIZATIONAL REVENUE (US$)

$5M - $24.9M	31%
$25M - $199.9M	16%
$200M - $499.9M	11%
$500M - $999.9M	6%
$1B - 10B	4%
$10B+	2%
Unable to disclose	30%

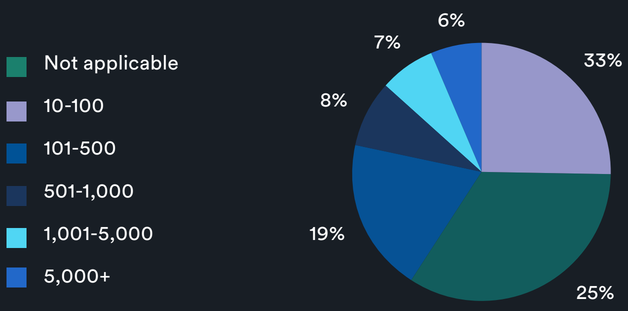
GLOBAL ORGANIZATION EMPLOYEE COUNT



PHYSICAL SECURITY DEPARTMENT EMPLOYEE COUNT

1-20 Employees	54%
21-200 Employees	29%
201-1,000 Employees	11%
1,001-10,000 Employees	5%
10,000+ Employees	2%

VIDEO SURVEILLANCE DEPLOYMENT (# OF CAMERAS)



ACCESS CONTROL DEPLOYMENT (# OF CARD BADGES OR TOUCHLESS ACCESS READERS)

Not applicable	36%
1 - 20	13%
21 - 200	13%
201 - 1,000	14%
1,001 - 5,000	10%
5,001 +	14%

BACK TO TABLE OF CONTENTS

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:

Does your organization deploy other types of physical security infrastructure?

- Alarms
- Audio
- Automated barriers
- Automated control parking
- Biometrics
- Bollard barriers
- Boom barriers
- Building management systems
- Drones
- Electric fences
- Emergency Alert System (EAS)
- Explosives detectors
- Fingerprint recognition
- Fire detection and repression systems
- Floodlights
- Lidar
- Luggage scanners
- Metal detectors
- Mobile radios
- Radar
- Real-time locating system
- RFID asset monitoring
- Turnstiles
- X-ray systems

Were there any other reasons that led your organization to begin using the cloud for physical security applications?

- Ability to unify products and share system feeds with CI Partners/Law enforcement
- Cloud storage Is more secure and convenient
- Compliance with Government regulations
- Data security
- Earn security certification by national security guidelines
- Ease of use
- Fear of NVR theft
- Prevent the loss of recorded data if hardware is stolen
- Recording redundancy/backup
- Reduction of IT staff/IT salaries
- Sector regulations
- Shortage of IT personnel
- Small capex required
- Speed of access to files

Has anything else slowed your organization's adoption of cloud-based solutions for physical security applications?

- Access to sufficient bandwidth
- Cloud-stored data no longer belongs to you, needs a data steward to use it
- Connectivity problems
- GDPR
- Lack of culture for using technology
- Power outages

Are there any other reasons that deterred your organization from deploying security solutions to the cloud?

- GDPR
- Lack of sufficient space in our data center
- Prohibited for Critical Infrastructure

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

- Drones
- Electronic Article Surveillance
- Fire detection and suppression
- IoT asset management and tracking
- Logistics inventory control
- Panic buttons
- Third-party integrations that offer less energy consumption
- Traffic violation

BACK TO TABLE OF CONTENTS

Select the top 3 challenges faced by your organization in 2022

- Budget constraints
- Changes in government policies
- Long delivery times
- Material shortages
- Power consumption
- Regulations
- Rising costs

What kind of HR challenges affected your physical security department in the last year?

- Constant movement/reassignment of personnel
- High inflation rates and increasing salaries
- Lack of budget to provide training

What new processes or priorities were activated by your organization this year?

- Applications development
- CRM/ERP change
- Fire safety system
- Reduction of emissions by 2025
- Remote working

What capabilities did you prioritize in the last year?

- Access control
- Cybersecurity
- Face recognition
- Fire detection and suppression
- PSIM
- Video analytics
- Wildlife GPS monitoring

What kind of projects has been affected? (by delays caused by supply chain issues)

- New installations/projects
- Office moves

How did you respond to delays caused by supply chain issues?

- Hired equipment from a subcontractor
- Increased inventory
- Purchased earlier

Which cybersecurity and data protection capabilities have you recently implemented over the last year?

- Information system audits
- ISO27K certification
- Isolated VLAN for IOT security devices
- Operating contingent plans
- Outbound communications only
- VPN
- Whitelisting specific IP addresses and communication ports

Are there other remote capabilities that are frequently requested by your customers?

- Access control monitoring
- Access to GIS based maps
- Activate and deactivate
- Alerts to messaging platforms such as Telegram, Signal or Whatsapp
- Case management
- Data privacy
- Diagnostics and system health
- Electronic Asset Protection Systems (EAS)
- Geolocation
- Guard tour monitoring system
- HVAC integration control to the security system
- Integration with fire alarm systems
- Intercoms
- Live video sharing to third parties
- Logistics route control
- Nurse call
- Panic buttons
- Predictive maintenance
- Remote audio communication
- Remote maintenance
- Third party system management
- UAVS remote control
- Virtualization

BACK TO TABLE OF CONTENTS

Which solutions are your customers looking to invest in to advance or improve physical security deployments in the next 12 months?

- Emergency Alert System (EAS)
- Fire detection and repression systems
- Panic buttons
- People counting
- Object detection technology using radio waves to determine the interval, altitude, direction and speed of such objects
- Thermal detection
- Wildlife GPS monitoring

Which actions have you taken to mitigate hardware procurement and inventory issues related to the current supply chain challenges?

- Allow customers to pre-order prior to tender release
- Certain projects are simply delayed if there is no substitute
- Directing efforts to professional services and technical support
- Lengthened lead times
- Opened a repair center to bring back some easy to fix electronics into production
- Re-design systems
- Use second-hand equipment

Will other operations be affected by work on your deployment backlog?

- Access to finance
- All operations will be affected
- Cash flow, billing, income collection
- Cybersecurity care for remote work
- Electric and other utilities
- Environment safety
- Everything is linked
- Human Resources
- Logistics
- Maintenance contracts
- Manufacturing
- Operations
- Skilled staff availability
- Training on the new brands that we incorporate into the solution portfolio has been delayed

BACK TO TABLE OF CONTENTS

About Genetec

Genetec Inc. is an innovative technology company with a broad solutions portfolio that encompasses security, intelligence, and operations. 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