Physical Security in 2021:

Pivoting to meet new operational requirements

Research insights from over 1,500 physical security professionals

Genetec™

March 2021

Contents

About the research

In January 2021 Genetec EMEA surveyed physical security professionals based in Europe, Middle East and Africa. Following a review of submissions and data cleansing, 1,550 respondents were included in the sample for analysis.

Some details about the survey methodology

The target population for the survey focused on individuals working for organisations participating in the procurement, management, and/or use of physical security technology. The target population included Genetec end users, integrators and consultants, participants contacted directly by third-parties via opt-in email lists and those who responded to invitations to complete the survey on social media.

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

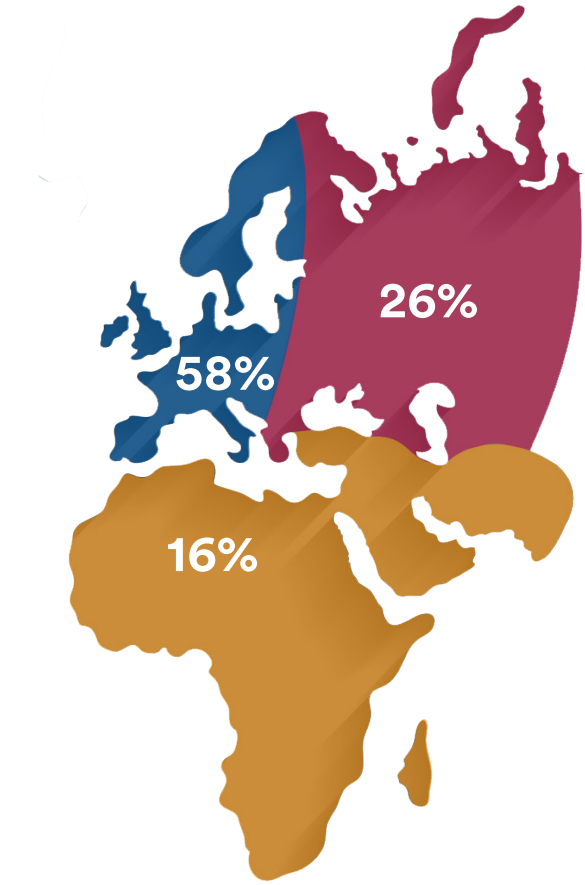
INDUSTRY BREAKDOWN

Public Sector
26%

Enterprise
47%

Retail & Financial Institutions
27%

REGIONAL BREAKDOWN



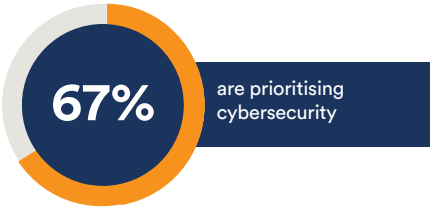
Executive summary

Physical security teams are accustomed to anticipating and responding to the unexpected. Yet, 2020 was a year like no other. In the face of a global pandemic, security operators have played a frontline role in protecting the health and well-being of communities. They have gone above and beyond, optimising the security of facilities and introducing new processes to address the challenges produced by COVID-19.

In this research, we report on the thoughts of 1,550 physical security professionals and take a closer look at how they are balancing shorter term needs with longer term priorities. These findings offer insight for physical security teams as they develop their organisations' own infrastructure and security strategies.

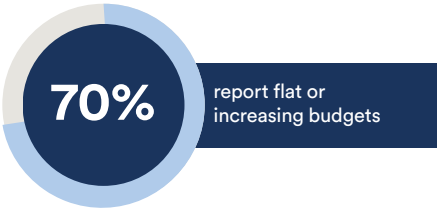
1 Cybersecurity is a strategic priority for 2021 and beyond

The emergence of new cyber threats as a result of the pandemic is well documented. ENISA – the European Agency for Cybersecurity – has highlighted the weakening of existing cybersecurity measures through changes in working and infrastructure patterns[1]. Against this backdrop, 67% of respondents are planning to prioritise the improvement of their cybersecurity strategy in 2021.



2 2021 budgets are being maintained or improved

Despite wider fiscal pressures the majority of respondents see the digital transformation of security and operations as a critical activity. This is reflected in 70% of respondents reporting that operating budgets will stay flat or increase in 2021.



3 Video, Analytics, Access Control and Identity Management viewed as enabling technologies

The realities of COVID-19 have emphasized the value of technology in providing greater insight, control and understanding of how and when facilities are being used. With the potential to improve people flow and streamline security operations to comply with local regulations, video analytics, access control and identity management were all identified by respondents as strategic technologies for 2021.

1.https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

Key findings

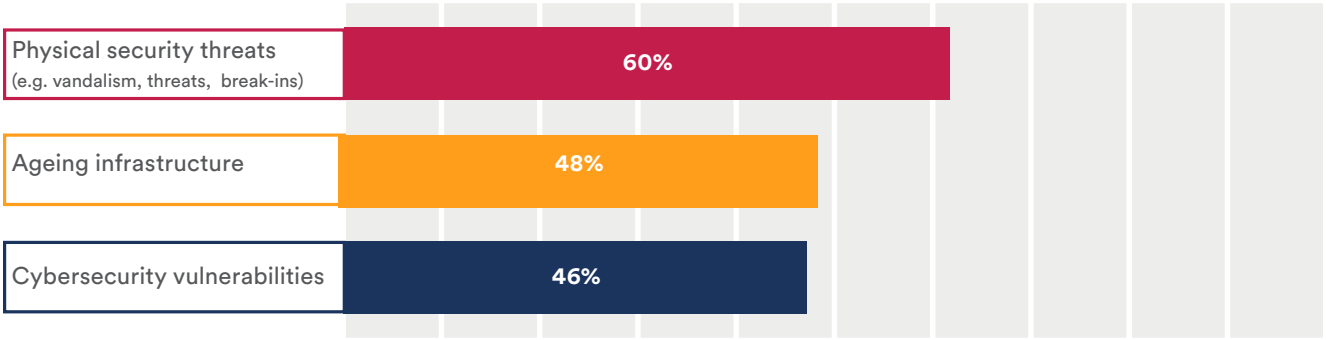
2020 has refocussed priorities

The challenges faced in 2020

In 2020, physical security practitioners dealt with a wave of restrictions greatly impacting their work, limited access to operational tools, and an environment in which criminals saw opportunity to exploit our move to work from home. Ageing and legacy systems struggled to connect remote employees to the office putting a sharp focus on underlying infrastructure inefficiencies and the need for new technology to support the new reality. – while empty facilities posed a new remote management risk for physical security teams.

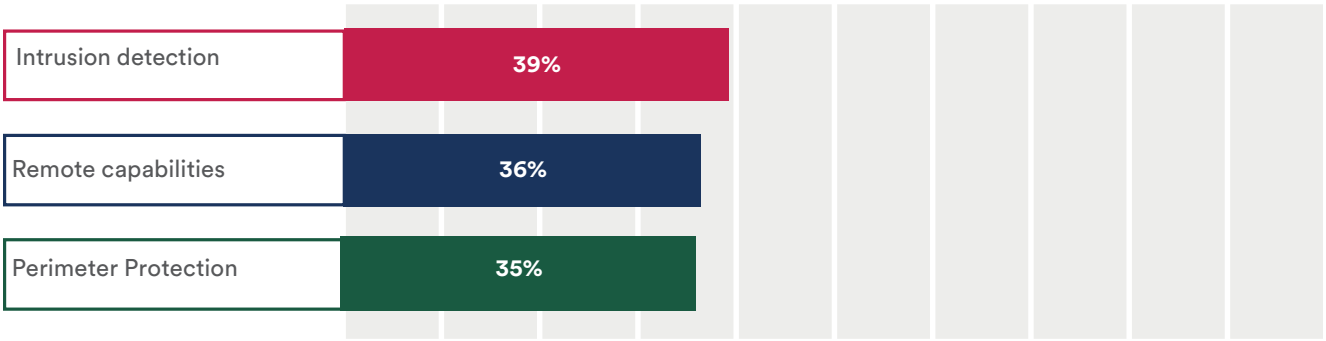
THE TOP THREE CHALLENGES FACED AS A RESULT OF THE PANDEMIC

Respondents could select multiple options



Intrusion detection, perimeter protection and remote capabilities all help to address new requirements for the management and monitoring of people and facilities. These technologies were all commonly deployed in 2020 to support lockdown operations and an eventual, progressive return to work.

TECHNOLOGIES DEPLOYED IN RESPONSE TO THE CHALLENGES OF COVID-19



Existing systems help transform operations

The innovative use and repurposing of existing security systems has proven invaluable in adapting to new ways of working. Users have leveraged existing video surveillance and access control systems to monitor occupancy levels, enforce new one-way traffic systems within a facility and even to remotely manage access to equipment stores or inventory. In each case, enhancing efficiency and streamlining operations.

42% **are leveraging existing systems to manage pandemic challenges**

Digital Transformation is picking up pace

Digital Transformation is altering all aspects of business operations. And while physical security departments have traditionally been slower to adopt the cloud, survey results indicate the situation is rapidly changing.

Pre-pandemic, just 37% of respondents identified as well underway in their adoption of cloud or hybrid cloud infrastructure for physical security. However, almost two thirds (64%) reported the pandemic as having somewhat (51%) or greatly (12.5%) accelerated their cloud strategy in relation to physical security.

In the midst of the short-term chaos, it could have been tempting to shelve or defer longer term decisions related to the evolution of an organization's security infrastructure. Yet, responses illustrate that with the quick evolution of the situation, and resulting need for supporting technology, the financial and resilience benefits of cloud versus on-premises deployments are being closely evaluated.

While 76% of respondents saw some projects delayed in 2020, only 8% reported projects being cancelled. The results suggest cloud adoption will proceed at pace in 2021 and beyond.

37%

are on cloud or hybrid cloud

50%

report that the pandemic is accelerating their cloud strategy specifically in physical security

50%

have deployed hybrid cloud solutions to manage physical security operations

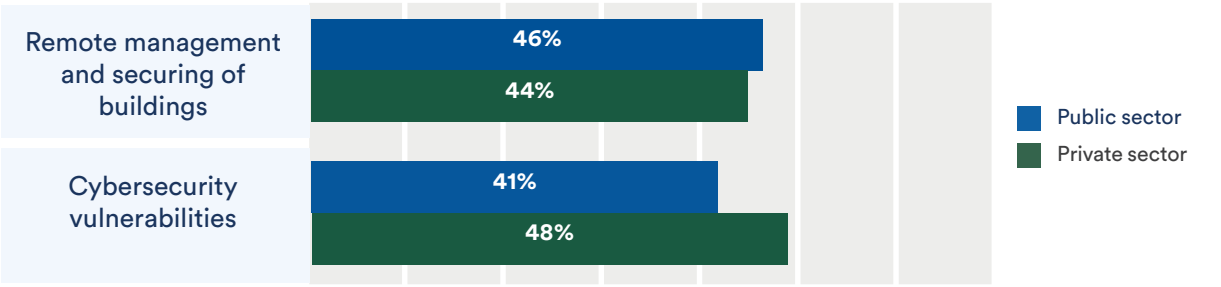
Key Regional & industry findings

A breakdown of our findings by industry and region points to the truly universal disruption, challenges and requirements created by the pandemic. COVID-19 makes no allowance for the sector or territory in which an organisation is operating. The most notable finding of the report is the near unanimous agreement across all categories of the core challenges, key technologies and 2021 priorities.

In terms of small differences, the below charts point to interesting variations between sectors and regions.

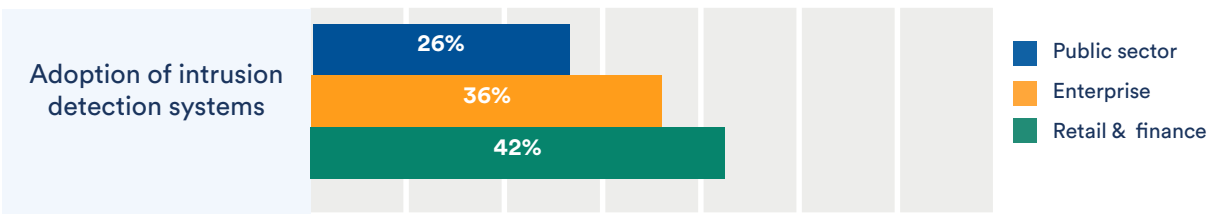
INDUSTRY FINDINGS

Public sector organisations were the only segment to view the remote management and securing of buildings as a bigger challenge than cybersecurity vulnerabilities as a result of the pandemic.



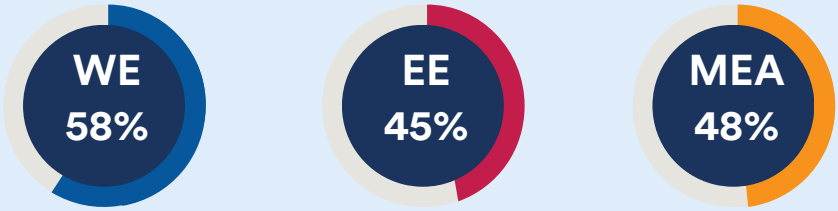
Private sector organisations are adopting video analytics more enthusiastically, than their public sector counterparts. However, the public and private sector are closely aligned on almost all other technologies.

Retail & finance institutions are the most likely to have introduced new intrusion detection capabilities during lockdown.

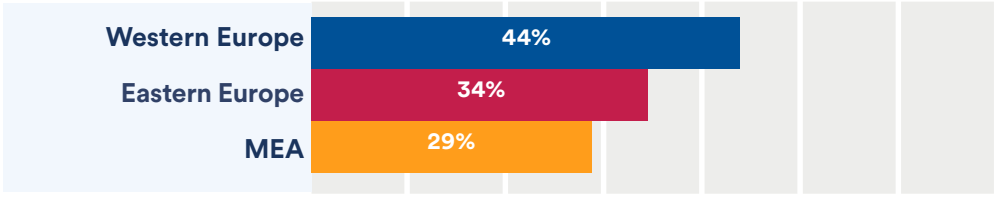


REGIONAL FINDINGS

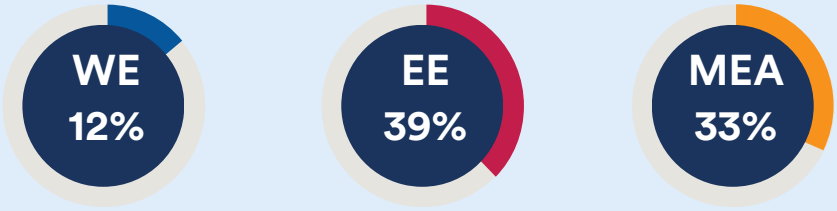
Implementing better business continuity plans is a particular concern for organisations in Western Europe:



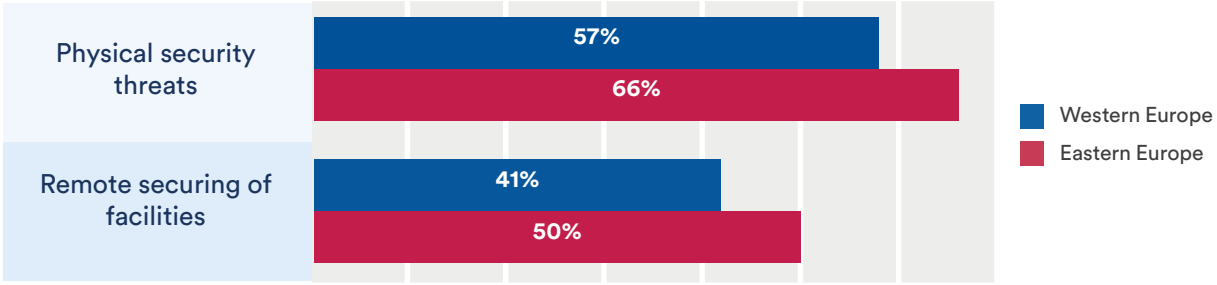
Western European respondents are moving faster in the adoption of video analytics.



Perimeter protection has been much more readily adopted during lockdown in Eastern Europe and META than it has by organisations in Western Europe.



Eastern European respondents were the most concerned about physical security threats and the remote securing of facilities



Takeaways for 2021

1 Embrace the Cloud

In 2020 Cloud technology proved invaluable in enabling organisations to quickly adapt to large scale remote working and the transition of business practices online. Looking ahead, businesses and governments will continue to expand their cloud adoption and it is imperative physical security capabilities evolve at the same pace.

Cloud and hybrid cloud systems offer advantages such as data protection, system flexibility, performance and cost savings. They encompass near-term enhancements such as greater scope for monitoring and longer-term opportunities such as the addition of new functionalities. There is no one-size-fits-all, each organisation should explore the possibilities based on its own specific requirements. For those just beginning this journey hybrid cloud is a good place to start the transition.

2 Focus on cyber resilience

Cyberattacks are inevitable and physical security systems are a known to attack surfaces that can offer an entry point to an organisation's network and data. Furthermore, all the signs point to cybercrime continuing to escalate in 2021 with the rise of work-from-home and the growing adoption of IoT.

This convergence of threats means cyber and physical security measures can no longer be treated as separate conversations. It is time for physical security professionals to proactively partner with their counterparts in IT to understand the true limits of the security perimeter and work to develop strong governance and processes to mitigate against cyber-attacks. This requires a twin focus on cyber hardening existing systems and practicing good cybersecurity hygiene when adding new technologies.

3 Build Security Operations on a Unified Platform

If there's one key lesson to take from 2020 it is just how quickly an evolving situation can challenge the very fundamentals of our operations. Yet one constant is the strengths of a unified platform in providing actionable insight and ensuring the necessary agility to respond. The last thing needed in a crisis is blind spots and workarounds for siloed systems that don't communicate.

Security systems must be resilient enough to work on the days where nothing happens and the days where everything happens. They must have the ability to grow and evolve as needed in line with the new challenges that the organisation face. They must also allow data from many different sources to be intelligently combined, qualified and visualised so that operators can truly understand, master and respond to what is happening within their environments.

Appendix

Appendix 1 – Survey methodology

Genetec Inc. surveyed physical security professionals in January 2021. The goal of the research was to:

- Find out how physical security departments across EMEA are leveraging technology to meet short term needs and long-term priorities.

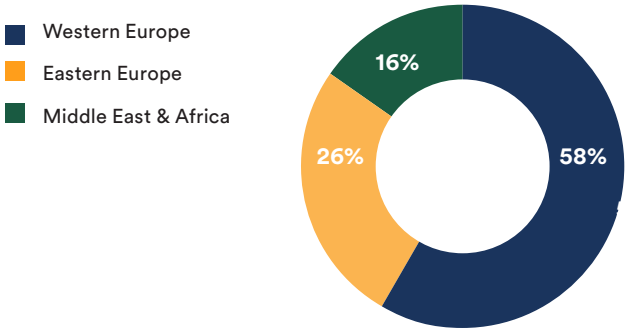
Following a review of submissions and data cleansing, 1,550 respondents were included in the sample for analysis.

The target population for the survey focused on individuals working for organizations participating in procurement, management, and/or use of physical security technology.

- Survey samples were run across all regions in EMEA.
- The target population included Genetec end users and participants contacted directly by email and social media channels.

Appendix 2 – Survey demographic information

GEOGRAPHIC REGIONS



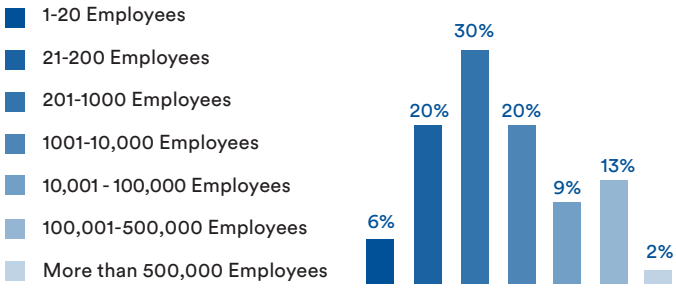
INDUSTRY GROUP

Enterprise	47%
Public Sector	26%
Retail & Finance institutions	27%

INDUSTRIES

Airports	7.62%
Energy and utilities	9.94%
Federal government	2.32%
Financial institutions	14.13%
Gaming	4.93%
Healthcare	8.89%
Hospitality	4.71%
Local government or cities	2.54%
Manufacturing	15.70%
Parking enforcement	4.11%
Public safety	8.97%
Public Transit	3.21%
Retail	5.98%
Sports and venues	1.94%
State government	2.69%
Traffic management	2.32%
Grand Total	100%

ORGANISATION EMPLOYEE COUNT



PHYSICAL SECURITY EMPLOYEES

1-20 Employees	17%
21-200 Employees	38%
201-1,000 Employees	27%
1,001-10,000 Employees	16%
More than 10,000 Employees	3%

About Genetec

Genetec™ develops open platform software, hardware and cloud-based services for the physical security and public safety industries. Its flagship product, Security Center, unifies IP-based video surveillance, access control, and automatic license plate recognition (ALPR) into one platform.

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

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