



2022

TOP SECURITY TRENDS

Hybrid Work Fuels Cloud-based Access Control Demand



INTRO

Historically, security has been oriented around guards, fences and other measures to keep the bad guys out. But in today's environment, access control is much more than that. Today, access control is the enabler for the digitization of the built world and expanded Proptech ecosystem. Organizations expect technology to add value via data—to provide business insights, generate new revenue streams, create efficiencies, understand user behavior, document trends, more efficiently allocate human capital and so on. Cloud-based access control systems, especially when they are integrated with other security and Proptech systems and features, provide a rich, largely untapped source of data.

The findings in this survey hint at just a fraction of the potential for data capture, analysis, and monetization in cloud-based systems. For example, half of surveyed organizations are investing in hybrid workplaces, confirming the future is indeed having the ability to support hybrid work environments. Yet some organizations are increasing square footage, and the most common access control integration is visitor management. That intelligence can help organizations make better business decisions, involving such areas as business travel, lease negotiations, and capital investments in technology. Those are a couple of possible applications of the data. We encourage you to actively use this report as a tool, for prioritizing and decision-making on all aspects of physical security in the structures you are responsible for or occupy.

Organizations are investing in hybrid workplaces, confirming the future is indeed having the ability to support hybrid work environments

Key Highlights

- 1 Hybrid work is here to stay
- 2 Data is the driving force behind change
- 3 Integrations are essential
- 4 Mobile access and credentials are growing
- 5 Cloud is the key to security centralization and enabler of the new work dynamic



TOP SECURITY TRENDS IN 2022

Hybrid work is here to stay, and access control is driving security and non security aspects of the hybrid work model, according to a survey conducted by Brivo on the state of security in 2022. Almost 60% of the 550-plus survey respondents currently use a hybrid work model, and nearly two-thirds report that access control is extremely or very important to that model. Further, 65% of respondents say that access control and its integration with other technologies have been very important or extremely important toward enabling a hybrid workplace since 2020.

Cloud migration underlies the trend toward access control becoming a cornerstone in a hybrid work environment. Forty percent of respondents have centralized their systems in the cloud, up from 35% in the [2021 survey](#). Another 31% are partially centralized, while 28% remain decentralized. Even those who do not use cloud-based security systems today understand the benefits: according 57% of respondents say that cloud-based access control would improve their security.

Brivo conducted the survey between January 6-28, 2022, in partnership with [ASIS International](#), drawing 557 responses from security and facilities professionals across two dozen industry sectors. Approximately 50% of the respondents came from Europe, Middle East and Asia, with the largest single set of replies from North America for the other half of the respondents. Sixty-one percent of respondents manage security for multiple facilities at the enterprise level.

65%

say access control integration with other technologies have been important to enable hybrid work

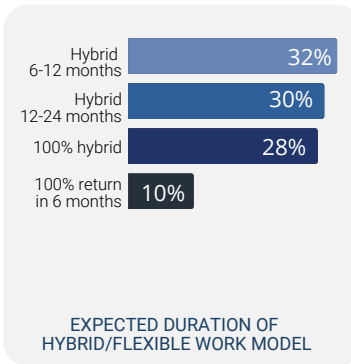
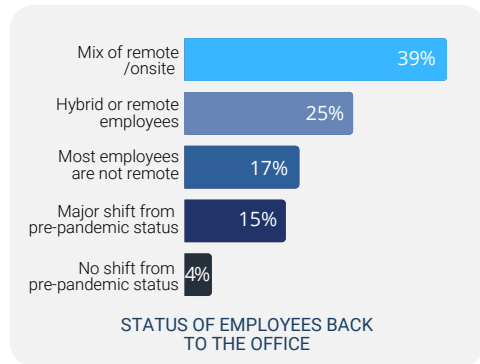
Hybrid work is here to stay, and access control is driving security and non security aspects of the hybrid work model



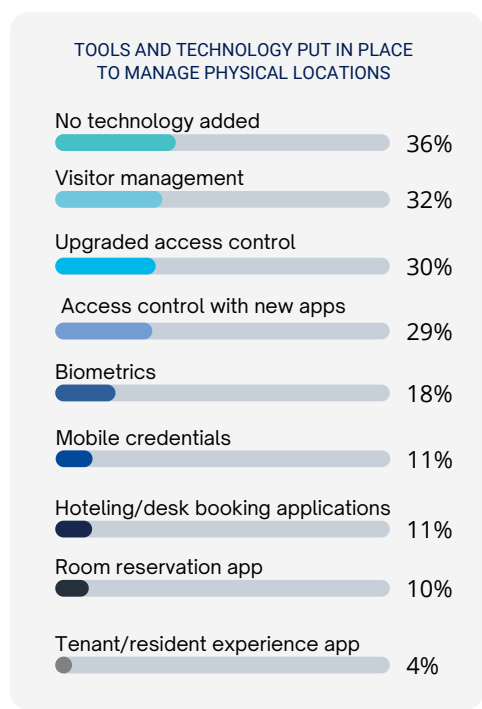
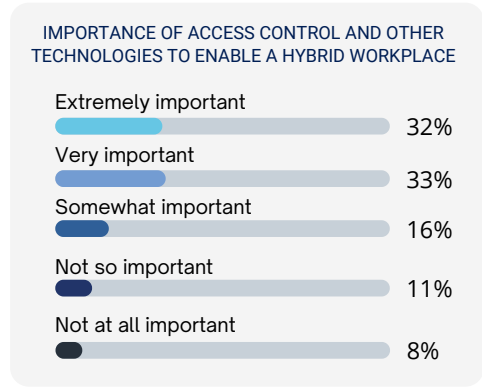
Hybrid Work is Here to Stay

THE HYBRID WORKFORCE IS HERE TO STAY

As the pandemic enters its third year, most organizations have evolved to a hybrid work environment — 58% of respondents currently operate a hybrid workforce, and only 10% expect to return to pre-pandemic work status within the next six months.

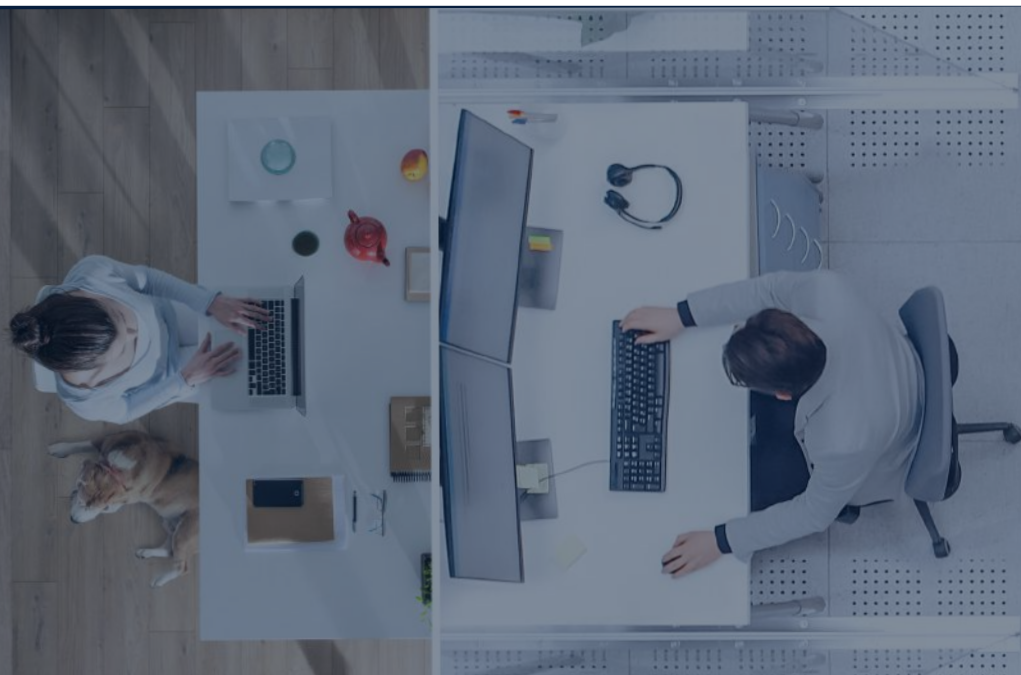


In fact, in the last six to 12 months, almost half of organizations have added technology to support a hybrid workplace, and as cited previously, almost two-thirds say that access control and its integration with other technologies have been extremely or very important toward enabling a hybrid workplace. The most common additions and upgrades include visitor management systems (32%), upgraded access control (30%), access control integrated with new applications (29%), and biometrics (18%). Several non security features appear as well: hoteling/desk-booking applications (11%), room reservation applications (10%), and tenant/resident experience apps (4%). Those non security features underscore the phenomenon of access control and other Proptech applications increasingly sharing the same platform.



58%

of respondents currently operate a hybrid workforce. Access control and its integration with other technologies have been extremely important toward enabling a hybrid workplace.

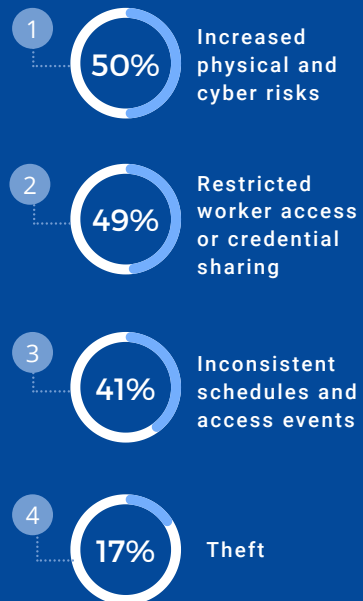


The big question on everyone's mind is what do office owners and tenants plan to do with their space? Many speculated that the pandemic was to be the end of the office and everyone will work remotely. Not all businesses can go to full remote status and many workers have articulated the benefits of working in the office to have more collaboration time with colleagues and a better rapport with managers and staff.

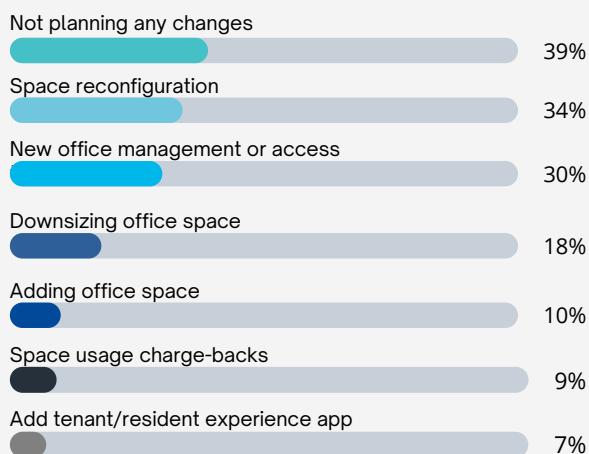
Adapting safety and security to the hybrid work environment entails more than just technology, and respondents identified other changes that their organization is poised to make in the next six to 12 months. While 39% don't anticipate any other changes, and 30% would lean on technological solutions, more than a third say that they will be reconfiguring their workspace. Notably, while 18% expect to reduce office space, another 10% anticipate adding space, which is good news for an uncertain commercial real estate market and runs counter to predictions of widespread downsizing of square footage.

The hybrid workforce presents special challenges of its own. Respondents commonly point to increased physical and cyber risks (49%), credential sharing, tailgating, or inappropriate access (49%), and inconsistent and unpredictable schedules and access events (41%) as significant pain points. Many of the additional responses indicated concerns related to isolated situations, such as mental health problems and lack of oversight.

BIGGEST SECURITY CONCERNS WITH THE HYBRID WORKPLACE MODEL



CHANGES ORGANIZATIONS ARE PLANNING TO ACCOMMODATE A HYBRID WORKPLACE



Adapting safety and security to the hybrid work environment entails more than just technology, respondents identified other changes that their organization is poised to make in the next six to 12 months

DATA LEADS THE WAY

Businesses are starting to realize the benefits of collecting security-related data. This data can be used to improve security, better understand space utilization and reduce costs. Yet, it is still true that a huge amount of the billions of data points that are created each day, like access events anomalous activities, video streams and images don't get collected, stored, or are only partially analyzed in traditional security systems.

Companies continue to grapple with how to best generate, harness and apply security data. That struggle comes across clearly in respondents' selection of their top physical security goal for 2022. The top objective: use physical security data—generated from events, video and intrusion detection to make informed business decisions. In fact, organizations cite various concerns surrounding security-related data: lack of actionable insight from data (33%), failure to generate sufficient data (23%) and incompatible data sources (16%). Close to 35%, however, say they face no challenges using or acquiring relevant data.

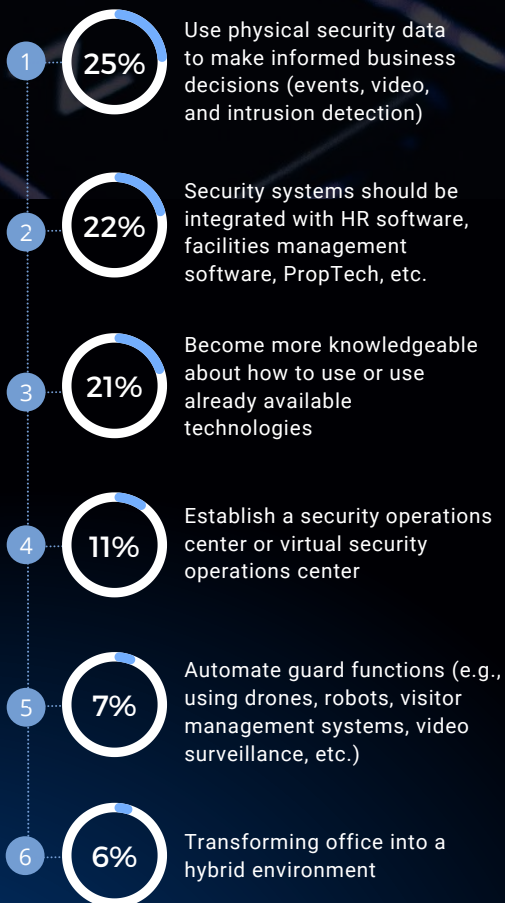
As to what benefits appropriate data would provide for their businesses, the plurality of respondents (38%) say that analytics would improve their physical security policies and procedures. Smaller numbers think that analytics would provide value for other departments, such as process, supply chain, and HR (16%), help staff investigate suspicious behavior patterns (15%), or support policy compliance (14%).

Beyond use and acquisition of security data, respondents desire several other physical security goals for 2022. Most prominently 22% plan to integrate security systems with other cross-functional areas within the organization (e.g., HR software, facility or property management applications, Proptech, etc.), and 21% aim to better understand how to use or leverage existing technology.

The benefits of using security related data is that it can be used to improve security, better understand space utilization and reduce costs

Data access and usage is a resounding theme in this year's survey. Many organizations are prioritizing data collection, analysis and reliance to make better informed decisions and set goals for their organizations.

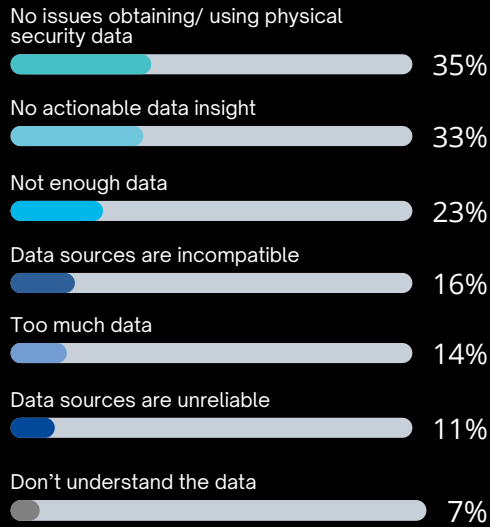
PHYSICAL SECURITY DATA GOALS FOR 2022



BENEFITS OF PHYSICAL SECURITY DATA USAGE FOR YOUR BUSINESS



ATTITUDES TOWARDS ACCESS CONTROL AND SECURITY DATA



The hybrid work phenomenon has not reduced the need for physical security and access control

Access control is even more important now as we create more fluid, open and hybrid environments

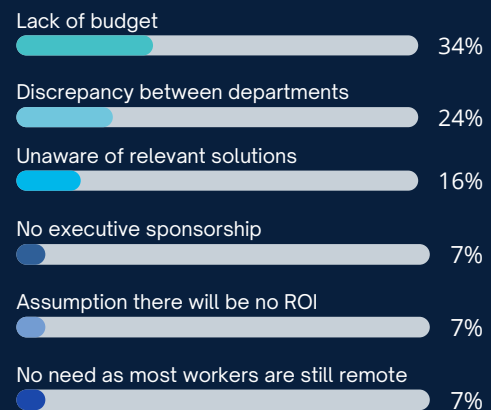
BARRIERS TO ADOPTION OF NEW PHYSICAL SECURITY TECHNOLOGY?

Security advances face long standing impediments. The most common barriers to implementing enhanced physical security include lack of budget (34%), lack of alignment between security and other departments (24%) and lack of understanding of currently available solutions (16%). This has not changed much over our previous annual surveys.

One interesting finding from the 2022 respondents was that very few respondents (7%) say they have little need for physical security because most workers are remote. Similarly, lack of ROI and lack of executive sponsorship (7%) highlights that while budget and inter-departmental barriers exist, executives understand the need for new security technology and have a clear line of sight into the return they can expect from their security technology investment.

These data points demonstrate that the hybrid work phenomenon has not reduced the need for physical security and access control. In fact, access control is even more important now as we create more fluid, open and hybrid environments.

BARRIERS TO NEW PHYSICAL SECURITY TECHNOLOGY ADOPTION



CONNECTIONS AND INTEGRATIONS CONTINUE TO PROMOTE ADOPTION

Integrations are connections that work together between systems and applications as a whole that share information and data. Integrating other systems and third-party apps amplifies the functionality and feature set of any platform.

Interoperability with other technologies can automate and enhance the capabilities of a solution that create business efficiencies and better user experiences. In the digital transformation era, centralized data across the near-endless technology ecosystem can help businesses make smart, well-informed decisions.

Respondents offered that the biggest barrier to adoption is interoperability with existing systems. When asked about interoperability and integrations, including which systems are most important to integrate with physical access control and security systems, respondents' answers fanned out fairly evenly among the 10 offered responses, led by video surveillance (22%) and identity and access management solutions (21%). Workplace management/hybrid working applications (13%) and visitor management applications (11%) registered the next two highest response rates.

Biggest barrier to adoption is the interoperability with existing systems

MOBILE ACCESS IS A GROWING BUSINESS OPPORTUNITY

Mobile solutions allow users to open doors, gates, and other entry systems with a smartphone. This makes navigating spaces in offices, gyms, garages, factories, schools and other places more convenient. The pandemic has accelerated mobile credential adoption by increasing the demand for a remote, contactless way of enrolling new people into access control systems as well. In addition, unlike physical cards or keyfobs, smartphones are more secure, easier to manage, and more cost-effective for business.

Mobile access control—combining the convenience and security of smartphones with the cost savings of eliminating keycards—has burgeoned as a consequence of clients' desire for touchless solutions during the COVID pandemic. Eighteen percent of respondents have already adopted that technology and another 42% are considering it. However, mobile credentials have not yet been broadly integrated across the enterprise.

60%

respondents are using or considering mobile credentials



Identity and Access Management



Video Surveillance



Mobile or Touchless Access



Remote Management



Visitor Management



Automated Software Updates



Shifting Systems Uptime and Cybersecurity



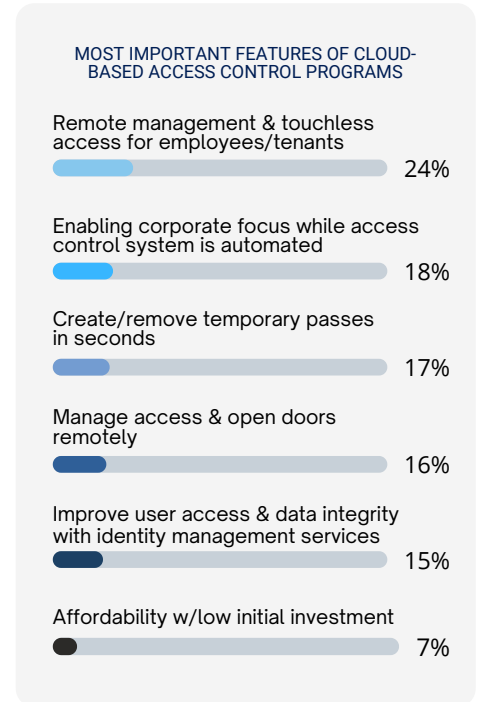
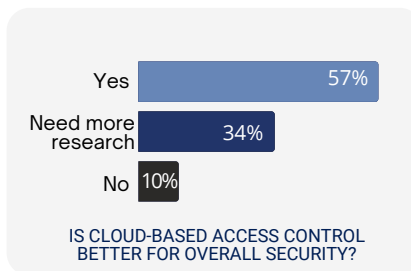
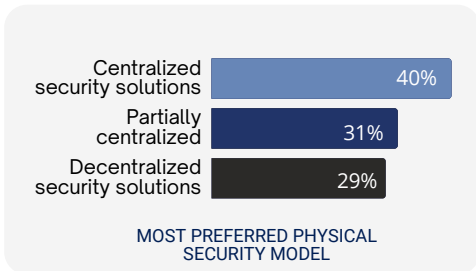
MOST VALUABLE FEATURES AND INTEGRATIONS OF PHYSICAL ACCESS CONTROL SOLUTIONS

CLOUD IS THE KEY TO SECURITY CENTRALIZATION

Cloud is essential to centralized security. As digital transformation has continued to modernize all aspects of business, the benefits of cloud-based access control have become more evident, particularly the lower total cost of ownership of the solution.

Additionally, cloud-based access control solutions enable easier integration with other cloud applications. Increased ease of integration means that the solutions can be more effective faster, starting on day one.

As previously cited, 40% of respondents have centralized their physical security systems in the cloud, up from 35% in last year's survey. And 57% of respondents say that cloud-based access control would improve their security.



The survey drilled into more specific aspects of cloud-based access control as well. When asked what were the most valuable elements of a cloud-based access control solution, respondents noted remote management and mobile/touchless access for employees and tenants as the top selections (23%). The second most valuable element (18%) was the ability for respondents to focus their time and effort on their business and leave the uptime, software updates and cyber security to their cloud-based provider. The third most valuable element respondents cited was the ability to assign or revoke credentials and issue temporary passes in seconds (17%).

Clearly the benefits of cloud-based access control has made a real and material impact on security and benefits are in contrast with on-premise solutions that cannot be managed remotely, deliver data insights or provide efficiency improvements.

40%

Have centralized their physical security systems in the cloud

57%

Think that cloud-based access control would improve their security



TODAY'S BIGGEST CHALLENGES

The survey population was asked to choose their top three common physical security challenges. Respondents most frequently selected physical security breaches (39%), executive buy-in to security priorities (35%), and staffing shortages (32%), mirroring last year's top challenges. Close behind those top three are loss/theft prevention (29%), staff training (29%), and compliance (26%).

Brivo's security suite, built on a robust, cloud-based access control platform, enables and optimizes hybrid work models, modernizes operations, and yields data that turn actionable insights into data-driven decisions across the enterprise ecosystem. Brivo's signature product, [Brivo Access](#), interacts seamlessly with the Brivo suite of security products, including [visitor management](#), [smart home automation](#), occupancy monitoring and [mobile management](#). It also offers an open API that integrates with an infinite number of features and applications, including identity management, elevator control, co-working and health and wellness.

Brivo systems generate a wealth of data for organizations to leverage. For a broader view of industry data and to access actionable insights, turn to Brivo reports, articles, surveys, blog posts, and other content. For deeper analysis, go to www.brivo.com to learn more.

TODAY TOUGHEST CHALLENGES IN PHYSICAL SECURITY RESPONSIBILITIES

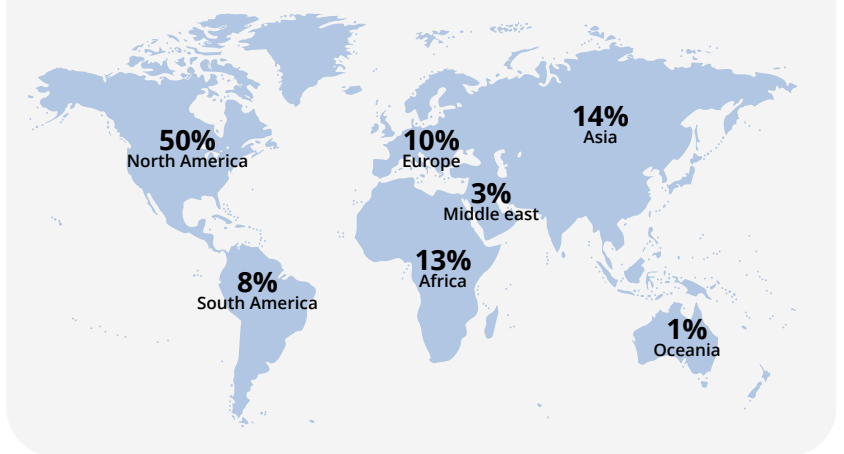
-Respondents chose up to three challenges-



Brivo's cloud-based access control platform, enables and optimizes hybrid work models, modernizes operations, and yields data that turn actionable insights into data-driven decisions across the enterprise ecosystem

Simply Better Security

Geographical distribution of survey respondents



Brivo, Inc., created the cloud-based access control and smart spaces technology category over 20 years ago and remains the global leader serving commercial real estate, multifamily residential and large distributed enterprises.

The company's comprehensive product ecosystem and open API provide businesses with powerful digital tools to increase security automation, elevate employee and tenant experience, and improve the safety of all people and assets in the built environment. Brivo's building access platform is now the digital foundation for the largest collection of customer facilities in the world, occupying over 300 million square feet across 40 countries. Learn more at www.brivo.com

Calculate Savings
by Moving to Cloud

calculate yours

Request a
Consultation

schedule it

Start Your Security
Upgrade Plan Now

upgrade here

visit brivo.com