2023 TOP SECURITY TRENDS

User Experience and Convenience are Driving more Effective Security

INTRO

Business today is about data: generating it, identifying it, culling it, collating it, analyzing it and monetizing it. Security is no exception. The thirst for data underlies the enthusiasm for adopting cloud-based solutions in the security environment. But data isn't the only hot trend in security in 2023.

In addition to harnessing the power of access data to make business decisions around energy optimization, facility expansion or contraction and much more, convenience and user experience have risen to the top of what is on security professionals' agenda this year.

How are security professionals addressing the user experience in physical security and prioritizing convenience? It could be the ease of passing through an access point using a mobile phone, one's face or license plate as a credential or the comfort of preheating a conference room to personal specifications.

As you will see in the following report, organizations increasingly realize that today's innovations go far beyond the block-and-tackle functions of legacy security systems. They represent significant developments throughout the business ecosystem—functions such as process efficiencies, supply chain management and sustainability—while also serving the need to secure spaces, buildings and lives.

Of course, driving these innovations are modern, cloud-based access control solutions. We continue to see the explosive demand and preference for cloud-based solutions in our surveys year-over-year as security professionals realize that to meet the changing physical space management demands, they need flexible solutions that can easily adapt and grow as the workplace continues to evolve.

The **experience** must be **easy** to **use**, **frictionless** and generate **value** for the business and the everyday user

2023 TOP TRENDS

1. User experience and convenience are driving the direction and adoption of new physical security technologies

2. Data collection and system integrations are no longer nice-to-have but business imperatives

3. Cloud-based access control with mobile and biometrics is moving mainstream

4. Cloud adoption and security centralization are accelerating

5. Security integrators need to stay ahead of technology or will get left behind

Convenience and **efficiency** are the **primary focus** of **modern security technology** to make security professionals' jobs easier

2023 TRENDS: A CLOSER LOOK

1 USER EXPERIENCE AND CONVENIENCE ARE DRIVING THE DIRECTION AND ADOPTION OF NEW PHYSICAL SECURITY TECHNOLOGIES

The Importance of User Experience in Access Control
Three years after the most significant shift from traditional working environments, workers have begun to return to the office, but the dynamics have changed.

It used to be that employees had to be on-site all the time, but now they expect flexible hours, hybrid environments, multiple accommodations and more conveniences. What were once non-negotiable expectations are now updated policies, procedures and processes to offer employees, tenants and residents more convenience.

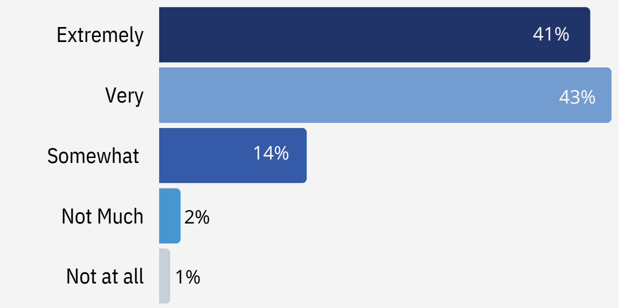
Nowhere is this shift more evident than in access control. Asked about the importance of user experience in access control, an overwhelming 84% said it was either extremely important or very important (see Graph 1).

84%
of respondents in 2023

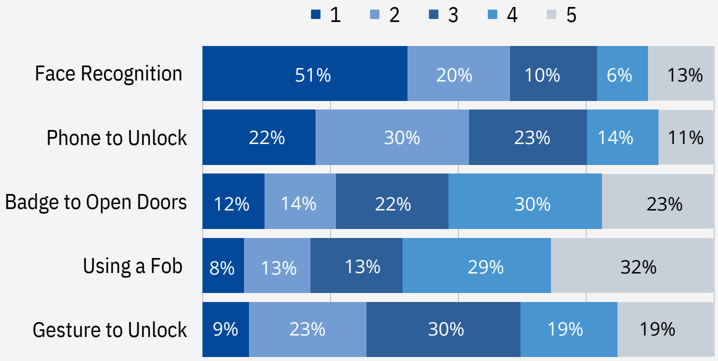
value access control user experience as significantly important

Security professionals are tuning into the convenience of passive, frictionless approaches largely driven by modern, cloud-based access control solutions. When respondents were asked to rank how easy it would be to use different types of access control, 51% and 22%, respectively, said that facial authentication or tapping a smartphone would be the most convenient (see Graph 2).

Security professionals are tuning into the **convenience** of **passive, frictionless approaches**



GRAPH 1 - IMPORTANCE OF USER EXPERIENCE IN ACCESS CONTROL



GRAPH 2 - RANK IN TERMS OF CONVENIENCE TO UNLOCK DOORS

Mobile access is not just building security

Car keys, boarding passes and tickets are an everyday experience that users enjoy and expect across all aspects of their lives

The **easier** you make it **for users**, the more likely they **will access** it **appropriately** without cutting corners, **improving security**

The adoption of these newer digital solutions and the desire to use technology is very high among security professionals. This makes sense because these digital actions are easier to record, measure and analyze once implemented in a physical security solution. Also, the easier you make it for users, the more likely they will access it appropriately without cutting corners, improving security.

Survey respondents also clearly saw convenience as the primary value proposition of another growing digital access control solution - mobile. Mobile access control rated far and above traditional plastic card or fob credentials: the two most common responses reflected the importance of the user experience (see Graph 3).

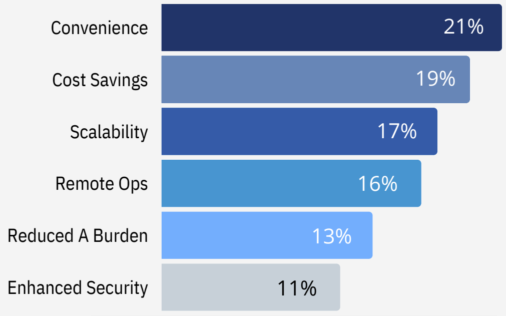
Sixty-five percent pointed to user convenience as a benefit of mobile access control, further supporting the argument that convenience in the user experience is an important factor in access control (see Graph 8). This is a trend not only in security but in other areas. For example, mobile car keys, boarding passes, concert and event tickets continue to proliferate. Users also expect that access at their places of employment will follow suit.

THE BIGGEST BENEFITS OF CLOUD SECURITY

Increased Convenience

Cost Savings

Scalability



GRAPH 3 - BIGGEST BENEFITS OF CLOUD ACCESS CONTROL

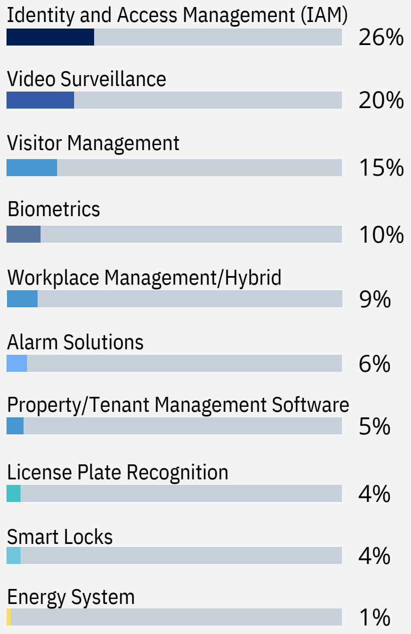
Employers are **rapidly adapting** their **offices** to meet the **demands** of **Millennial** workers' expectations for **convenience**

The Coming of Age of Millenial and Gen-Z as Users and Decision Makers

Workplaces have changed. That is well established starting before and accelerating during and post-pandemic. But this isn't a miraculous phenomenon. Changing workforce demographics is also a big reason employers need to update the work environment to meet the needs and wants of a workforce increasingly made up of Millennials and Gen-Z workers. Consider this: the U.S. workforce will comprise nearly two-thirds (64%) of Millennials or Generation Z by 2025 (LinkedIn).

Tenant- and workplace-experience apps are a growing trend in the enterprise and commercial real estate sectors and rank number 5 at 9% on the top integrations being implemented this year, behind video surveillance (20%), visitor management (15%) and biometrics (10%) (see Graph 4).

GRAPH 4 - MOST CRUCIAL SYSTEM TO COMBINE WITH PHYSICAL ACCESS CONTROL

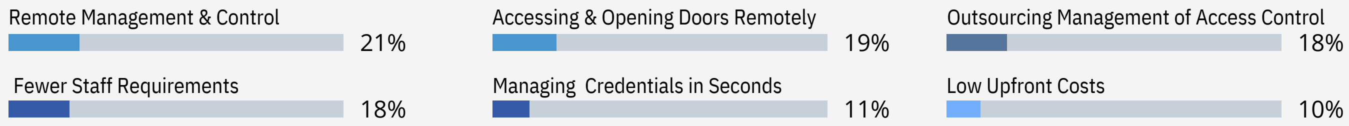


These apps allow employees to book rooms for meetings and presentations, change the temperature and lighting, find their way around large buildings, ask for maintenance, sign up for events, and even use a marketplace for services like dining, food delivery and package shipping.

While on the surface, these employee-experience amenities may not appear to be a necessary employee benefit. Yet employers are rapidly adapting their offices to meet the demands of Millennial workers and their expectations for convenience and mobile-derived services.

The theme of convenience also applies to security staff. When asked what problems cloud-based security can solve, security professionals listed a few that make their jobs easier, such as remote door management, instant creation, modification and revocation of credentials, and outsourcing the management and oversight of the access control system (see Graph 5).

GRAPH 5 - BIGGEST CHALLENGE CLOUD-BASED ACCESS CONTROL PLATFORM CAN HELP SOLVE



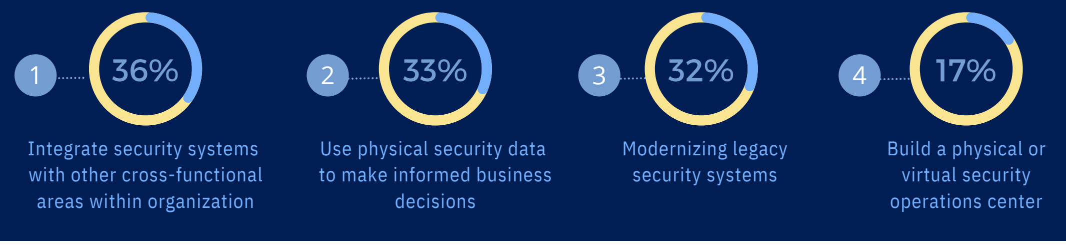
2 DATA COLLECTION AND SYSTEM INTEGRATIONS ARE NO LONGER NICE-TO-HAVE BUT BUSINESS IMPERATIVES

Previous Brivo Trends Reports have shown that cloud-based security environments collect and use data to improve efficiency, operations, and business strategy. This trend is growing as organizations:

- find new sources of data
- share data within the company
- extract data from existing sources
- improve tools to analyze data
- measure how to make money from data and
- proclaim the efforts to leadership and partners.

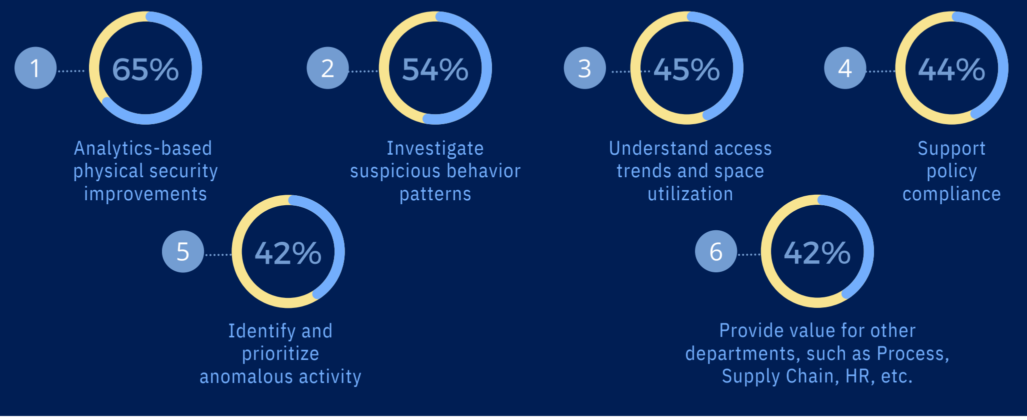
As in previous years, the number one security goal for 2023 (36%) was integrating security systems with other cross-functional areas within the organization, such as employee/tenant experience, proptech applications such as automatic lighting, human resources software and property management apps. The next most important goal for security professionals (33%) was using physical security data from sources like video surveillance and occupancy monitoring to make intelligent business decisions (see Graph 6).

GRAPH 6 - TOP FOUR PHYSICAL SECURITY DATA GOALS FOR 2023



A deeper indication in this year's survey results also reflects broadening uses for access data. As usual, data is desired to improve security and investigate suspicious behavior. Emerging use cases for access data include understanding access trends and space usage (45%), finding and prioritizing unusual activity (42%), and giving value to other departments like supply chain, process, and HR (42%) (see Graph 7). This trend shows that more security professionals understand the data sets that can be gathered from access control and how they can be used for more than just opening and closing doors to help make business decisions.

GRAPH 7 - BENEFITS OF PHYSICAL SECURITY DATA USAGE FOR YOUR BUSINESS



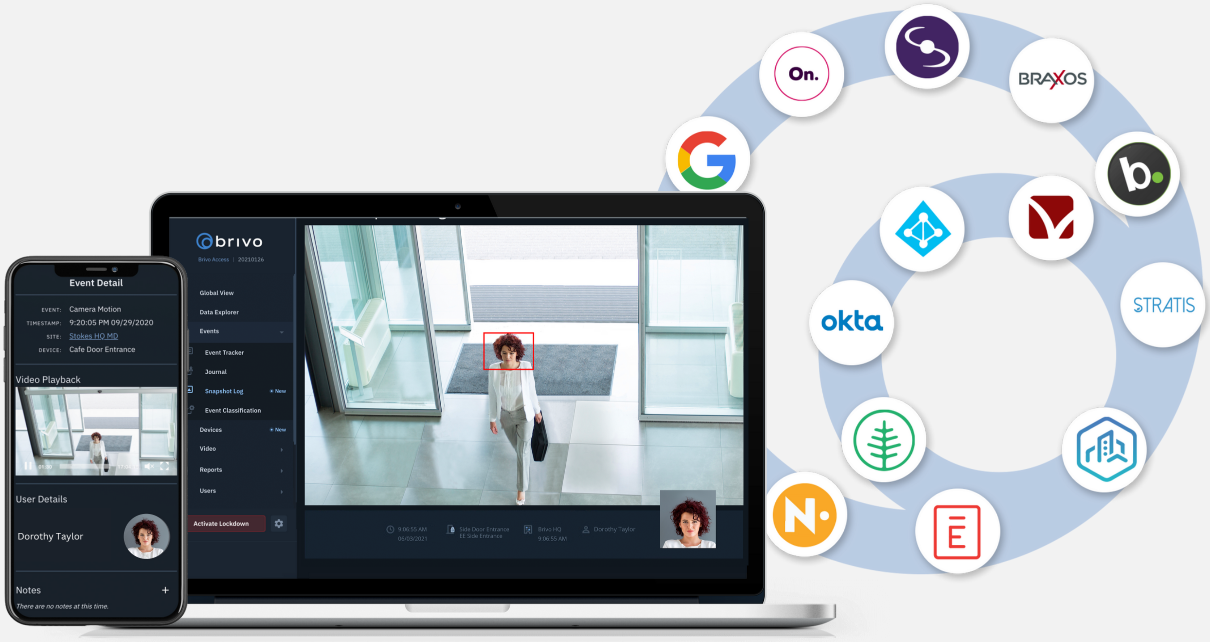
Integration is a Business Imperative

A trend we have seen repeatedly is the growth of integrations in the physical security space. Before the pandemic, the industry was talking primarily about integrations with video, intrusion and fire systems with access control. Now there are larger categories like identity management, workplace optimization, energy management, property management and tenant experience integrations, to name a few, that are part of the expanding ecosystems of a larger solution.

This year, respondents report a surge in access control integrations. The need for both increased security and enhanced convenience underlies this trend. Notably, the most frequent physical access control integration (36%) for 2023 is with identity and access management (IAM) - the cyber counterpart to physical access control (see Graph 4).

The popularity of integrating IAM solutions, such as those from Okta, Microsoft, and Google, shows the continued growth in connecting physical and digital security systems for added protection.

Identity management makes it easier for security teams to do their jobs using the same tool to manage all access automatically. Additionally, respondents clearly preferred access control methods that minimize the burden on staff. Solutions that eliminate manual tasks by syncing users across the two predominant types of corporate systems in any organization are of utmost importance to keep staff productive. As cyber and physical security increasingly rolls under a common Chief Information Security Officer's (CISO) purview, we will continue to see more system integrations between the real and cyber worlds.



Event Detail

EVENT: Camera Motion
TIMESTAMP: 9:20:05 PM 09/29/2020
SITE: Stokes HQ MD
DEVICE: Cafe Door Entrance

Dorothy Taylor

There are no notes at this time.

The popularity of **integrating** IAM solutions, such as those from **Okta, Microsoft, and Google**, **shows** the continued **growth** in **connecting** physical and digital **security systems** for added protection.

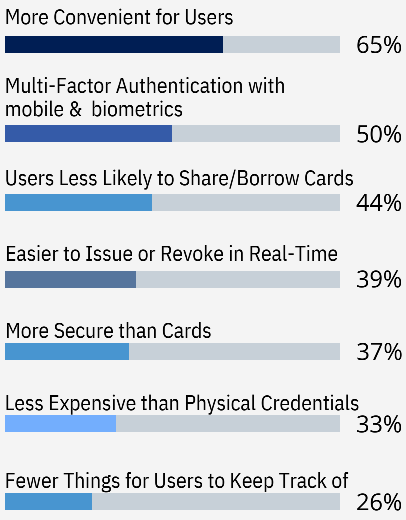
3 CLOUD-BASED ACCESS CONTROL WITH MOBILE AND BIOMETRICS IS MOVING MAINSTREAM

Today's fastest-growing access control solution leverages what almost everyone today keeps with them at all times: their smartphones. Physical keycards, tokens and fobs are far from gone, but their dominance may soon be history. Production and replacement costs, losses, thefts, loans and administrative burdens such as card issuances, modifications and revocations have long plagued organizations using physical credentials.

With smartphones, users receive electronic access to a mobile app from their employer, property manager or other authorized parties and register themselves at their convenience. Once registered, staff or residents can enter doors to which they are given access based on their role, time of day, or other factors.

Systems that use smartphones and biometrics get rid of many hassles and costs and can make security better as a whole. Enrollment, modification and revocation can be handled remotely and instantaneously. Users rarely or reluctantly lend out their smartphones and are much less likely to lose them than a generic plastic card.

GRAPH 8 - BENEFITS FROM USING MOBILE CREDENTIALS OVER TRADITIONAL PHYSICAL CREDENTIALS



FOR STAFF TRANSITIONING TO MOBILE ACCESS...

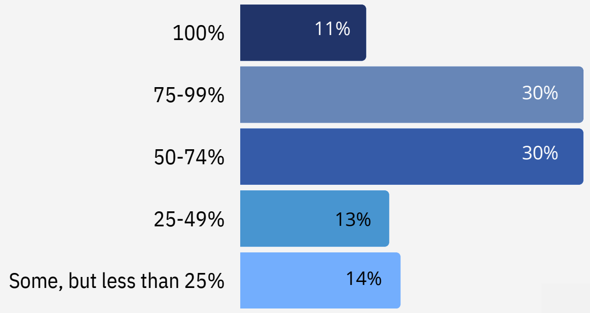
- Respects their time - they register where and when they want; no need to come to the office
- Respects their privacy - no biometric readers other than what they are comfortable using in their phones
- Respects their wallet - no charges for replacement cards
- Respects their need for convenience - changes in credentials are remote and seamless
- Meets them where they want to be - mobile first is already standard for applications ranging from car rides and dating to hotels and photography
- Scales to infinite uses - an access app can, or will soon be able to, do everything to register a visitor, book a conference room and request audio/visual support

FOR THE ORGANIZATION, MOBILE MEANS...

- No need/cost to print and distribute cards
- No need to replace lost cards
- Staff much less likely to lose or lend their phone, which increases security
- Multifactor authentication using biometrics in the phone (e.g., face recognition and fingerprints) adds security
- Staff and residents view mobile access as a positive gesture towards convenience and accommodation
- Administrators don't have to be in an office to issue a physical pass, they can more easily manage access and credentials from anywhere

The survey responses significantly substantiate these trends. Convenience is just one reason for mobile access adoption. Other benefits over keycards include user-friendly multi-factor authentication (50%), lower levels of credential lending (44%), easier issuance/modification/ revocation (39%), higher security (37%) and lower cost (33%) (see Graph 8).

In addition, almost three-quarters of respondents said that within three years, at least 50% or more of their users will have mobile access (see Graph 9).



GRAPH 9 - % OF USERS TO USE THEIR MOBILE DEVICE /CREDENTIAL/APP FOR CONVENIENCE IN THE NEXT THREE YEARS

Biometrics Interest and Adoption is Larger Than You Think

Biometric screening has been used in high-security situations for a long time. Still, it has now made its way into everyday life. Of those who deploy biometric solutions, 40% use them at all access points, not just doors into sensitive or high-value locations (see Graph 10). Biometrics is used as a primary access credential (37%) and a secondary credential for two-factor authentication (63%) (See Graph 11).

Biometrics emerged as a winner for limited high-security access applications. Facial authentication is the perfect plug-and-play application: all you do is show your face to a reader in an almost entirely frictionless way to gain access. There is nothing to remember, swipe or punch in.

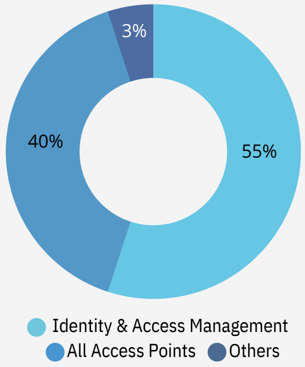
Facial authentication specifically showed increased interest and uptake as well. More than 60% of the people who answered the survey are considering adding biometrics to get into their buildings in the next three years (see Graph 12). Asked whether they would add face-based authentication if research showed that it was affordable and widely adopted, 80% said they were likely to do so—with 28% extremely likely to add that feature (see Graph 13).

+60%

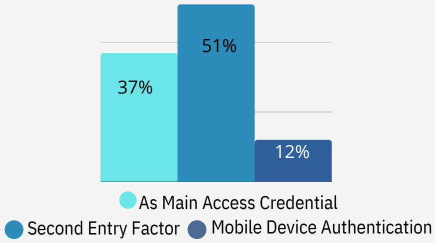
of respondents in 2023

are considering adding biometrics to their buildings in the next three years

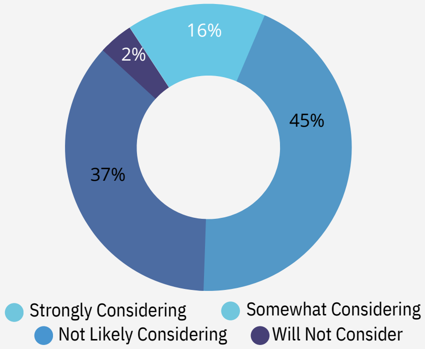
GRAPH 10- BIOMETRICS SCREENING USAGE

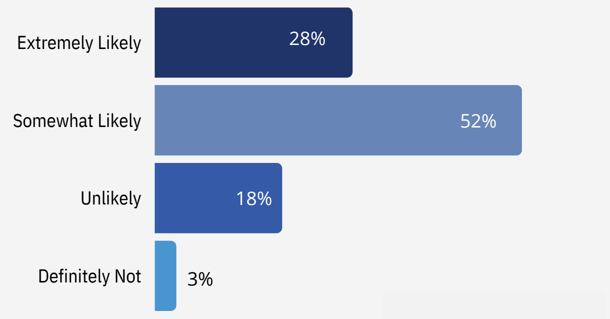


GRAPH 11- BIOMETRICS OR TWO-FACTOR AUTHENTICATION



GRAPH 12 -BIOMETRICS FOR FACILITIES IN THE NEXT THREE YEARS





GRAPH 13 - IF RESEARCH SHOWED AI AND FACIAL AUTHENTICATION AS MORE AFFORDABLE & ADOPTED, HOW MANY WOULD LIKELY CONSIDER USING IN THE NEXT THREE YEARS?

60% security experts predict that facial recognition is having the biggest impact over other technologies

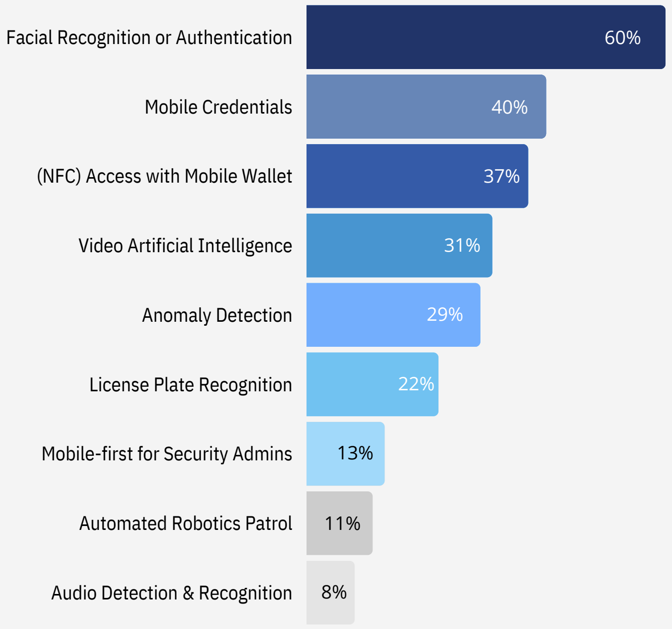
Biometric Pros

- Easy to use
- Credentials are personal and non-transferable
- Technology/costs have become affordable
- Easily integrates with other authentication methods

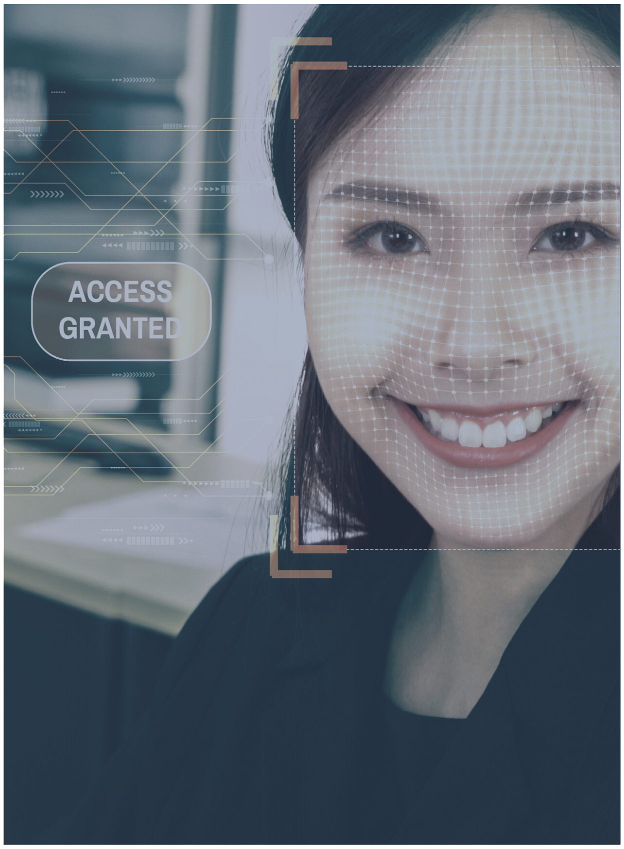
Biometrics Cons

- Personal data storage concerns
- Accuracy issues (false positives and negatives)
- Some technologies seem invasive (e.g., retinal scans)

Security experts were more bullish about facial authentication than any other credentialing, authentication, or access control technology. They predicted facial recognition (60%) as having the biggest impact over the next three years over such promising technologies as near-field communications and portable wallets (37%), video AI (31%), object recognition (22%) and audio identification (8%) (see Graph 14).



GRAPH 14 - ACCESS CONTROL INNOVATIONS WITH THE BIGGEST IMPACT OVER THE NEXT THREE YEAR



4 CLOUD ADOPTION AND SECURITY CENTRALIZATION ARE ACCELERATING

The Biggest Benefits of Cloud Security

Our research shows the preference and demand for cloud-based security solutions remain a consistent theme year over year. One of the most important benefits of cloud-based security frequently cited is that it makes things easier for users, and this is a theme that dominated survey responses this year.

The consumerization of IT has been happening across the business world for decades, but it is now starting to impact the security industry heavily.

Consumerization is the specific impact that consumer-originated technologies can have on enterprises. It reflects how enterprises will be affected by and can take advantage of new technologies and models that originate and develop in the consumer space rather than in the enterprise IT sector. Consumerization is not a strategy or something to be “adopted.” Consumerization can be embraced, and it must be dealt with, but it cannot be stopped (Gartner).

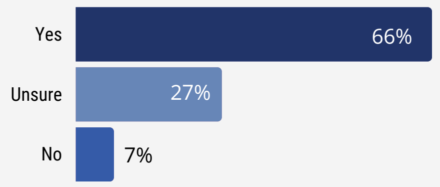
This phenomenon of unstoppable user-driven demand towards a consumer-like experience is spurring the disruption of traditional access control solutions. And it’s not just on the user side. We also see the demand for easy to manage solutions and integrated technology on the professional security side, heavily pushing the security industry to change.

Improving overall security is top of mind for respondents. In our 2022 report, 57% of respondents said cloud-based access control improved or could improve their overall security. That number jumped to 66% in 2023, with another 27% allowing for that possibility (see Graph 15). Cloud adoption and confidence in cloud-based security solutions are rapidly increasing. Survey respondents ranked benefits such as cost savings (21%), convenience (19%), increased security (17%), remote operations (16%), and the ability to scale up the platform (13%) as drivers when considering cloud access control (see Graph 16).

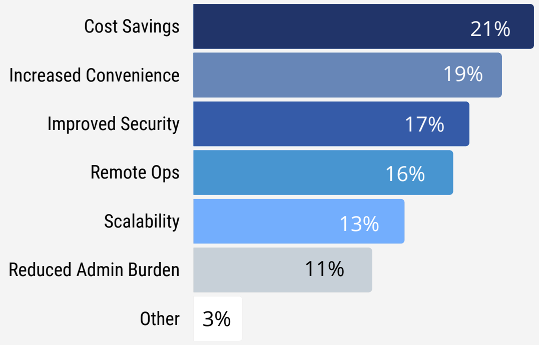
66%↑

of respondents in 2023

said that having cloud-based access control improved their overall security



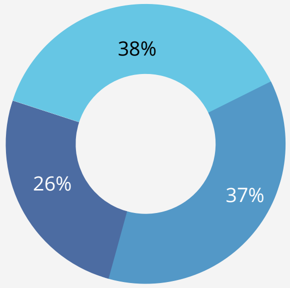
GRAPH 15 - CLOUD-BASED ACCESS CONTROL IMPROVES OR COULD IMPROVE YOUR OVERALL SECURITY?



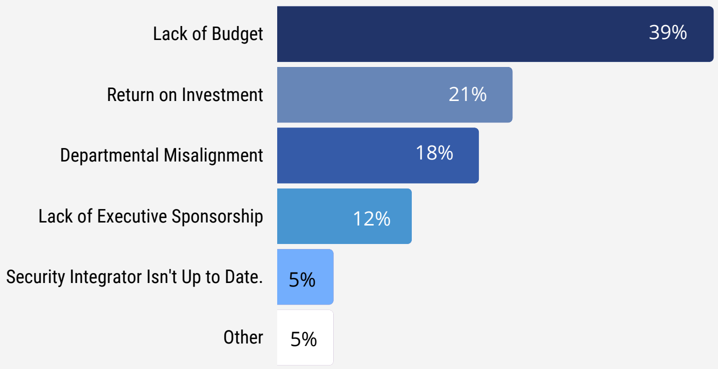
GRAPH 16 - MOST IMPORTANT BENEFIT OF CLOUD-BASED ACCESS CONTROL

Security centralization is another strong trend year over year. The number of respondents whose organizations are now partly centralized went up (38% compared to 31% in 2022) (see Graph 17).

That said, there are challenges to adoption. Respondents say that a lack of budget (39%) is the biggest reason they haven't adopted cloud-based solutions. Other barriers continue year over year, including the ability to show ROI (21%), demonstrating the clear benefits of cloud security is paramount in informing the executive suite to generate buy-in and influence budgets (see Graph 18).



GRAPH 17 - TYPE OF SECURITY MODEL



GRAPH 18 - KEY OBSTACLES TO MODERN PHYSICAL SECURITY TECHNOLOGIES

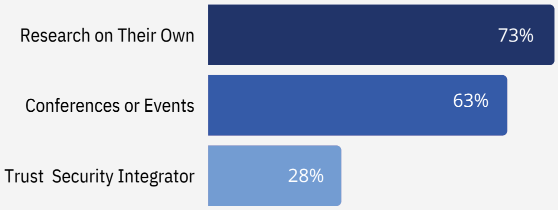
39%
of respondents in 2023

said a lack of budget is the biggest reason they haven't adopted cloud-based solutions

Finally, cloud benefits manifested themselves in security professionals' top security technology goals for 2023. Beyond generating usable data and adding integrations—discussed previously—respondents listed cloud-friendly goals such as modernizing legacy security systems (32%), building a security operations center (17%) and automating guard functions (15%) (see Graph 6).

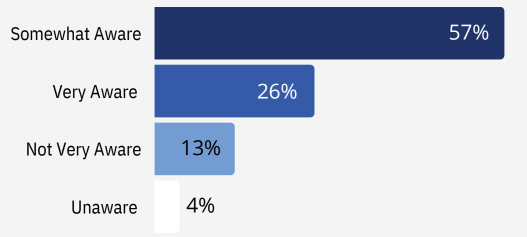
5 SECURITY INTEGRATORS NEED TO STAY AHEAD OF TECHNOLOGY OR WILL GET LEFT BEHIND

Staying up to date in a dynamic, rapidly changing industry is essential. It's not surprising that 73% of people who buy security do their own research on vendors and technology and that 63% of people who buy security attend conferences or other events to help them make decisions. So it isn't any surprise that only 28% rely on their security partners for that information (see Graph 19).



GRAPH 19 - HOW TO DISCOVER NEW PHYSICAL SECURITY TECHNOLOGY AND ITS BENEFITS

Going further, when we asked about the level of knowledge that their security integration partners have about the latest trends, technology and evolutions in the industry, the surveyed security professionals said that only 26% are up to date with cutting-edge tech. Nearly 60% of respondents considered integrators only somewhat knowledgeable, and 13% dismissed them as not knowledgeable (see Graph 20). This should be a wake-up call for security integrators to step up their game.



GRAPH 20 - WHICH OF THESE BEST DESCRIBES YOUR INTEGRATOR REGARDING LATEST TECHNOLOGY

The sobering conclusion of the above findings suggests that it has never been more important for the integrator community to advance their industry knowledge. It is critical that integrators understand the latest trends and shifting demands of users and stay on top of the latest advancements in cloud security. But they also need to train their teams to give better service and get back to consulting with their customers. As the security world gets smarter and more cloud-based, security integrators who are well-informed and educated will have a clear advantage in the market.

> As the security world **gets smarter** and more cloud-based, **security integrators** who are **well-informed** and **educated** will have a **clear advantage** in the **market**

What These Trends Mean for the Future

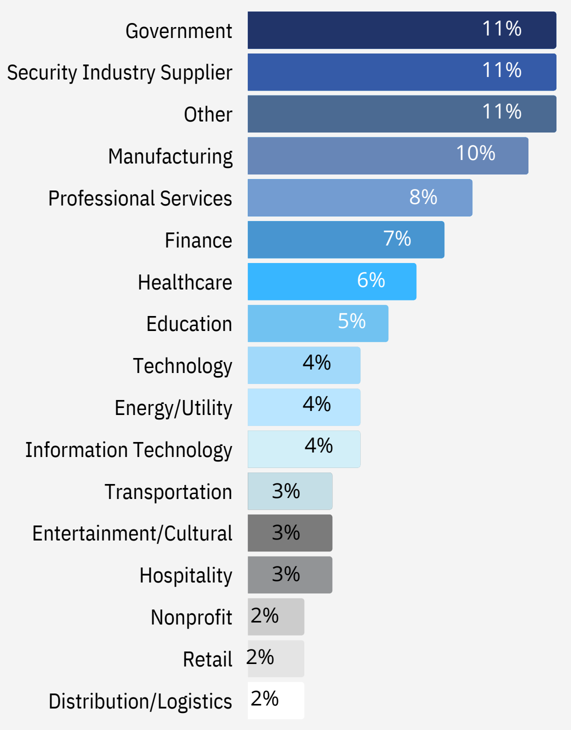
The voice of the end user and what they expect from a security solution was the loudest in this survey. Easy and convenient is expected-much like everything they use in their daily lives on their smartphones. Fortunately, there are also signs from the security industry professionals surveyed that they get it - they are looking to prioritize those consumer-like features while enhancing security.

The survey, now in its 6th year with these 2023 results, continues to show cloud adoption and interest in cloud adoption of access control security solutions remaining on the rise. As pointed out in Trend 4, 66% of respondents said cloud-based access control improved or could improve their overall security compared to 57% in 2022. But executive buy-in remains a challenge when prioritizing cloud-based access control security solutions.

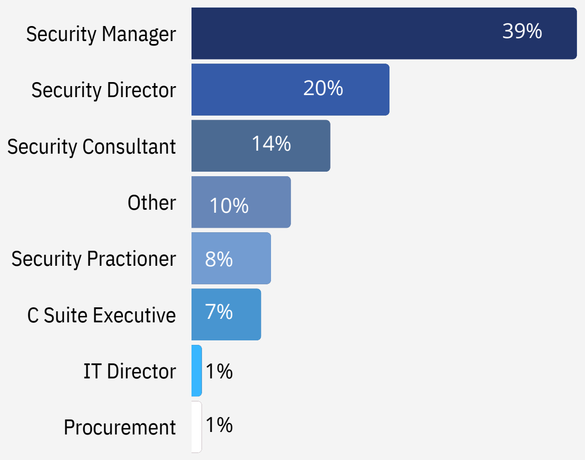
One of the primary purposes of this trends report is to provide those end users and security professionals data to accelerate decision-making. In today's world of cloud dominance, cloud-based access control security needs to be considered a must-have rather than a nice-to-have to achieve the experience expected from end-users and security professionals alike.

About The Survey

Conducted in partnership with ASIS International between October 1 and December 1, the 2023 Top Security Trends Survey drew 677 responses from security and facilities professionals across two dozen industry sectors. Over 50% of the responses came from North America, with the rest of the world accounting for the other half. Fifty-nine percent of respondents manage security for multiple facilities at the enterprise level.



GRAPH 21- PARTICIPANT INDUSTRIES



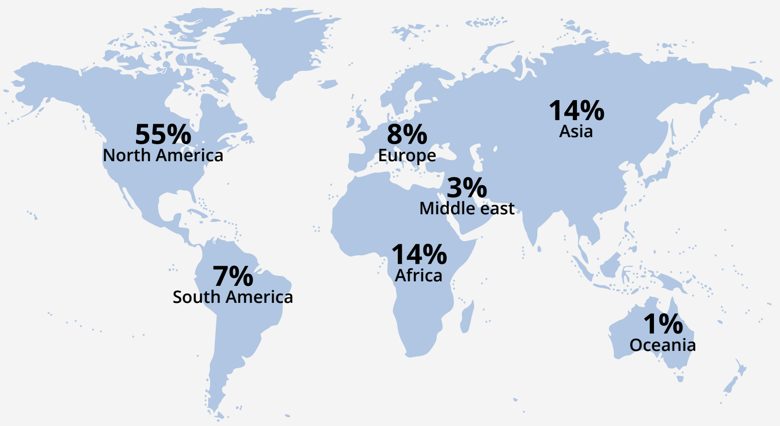
GRAPH 22 - PARTICIPANT JOB POSITIONS

677 security **experts** from all around the world participated in the survey and provided their comments

ABOUT BRIVO

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 a 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, protecting over 450 million square feet across 60 countries. Learn more at www.brivo.com.

Calculate Savings by Moving to Cloud

calculate yours

Request a Demo

schedule it

Start Your Security Upgrade Plan Now

upgrade here

visit brivo.com

brivo

1.833.462.7486 | brivo.com