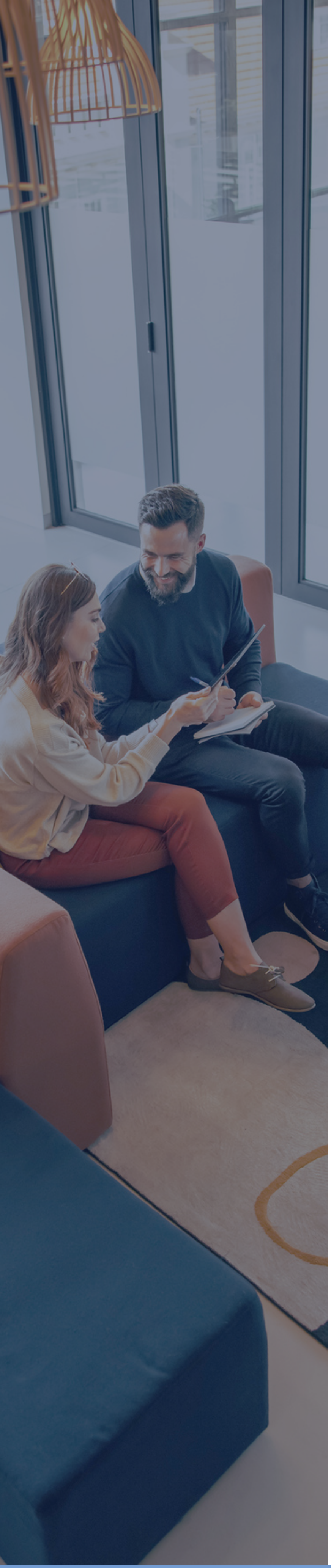
Shifting Boundaries

Managing Security in the Age of Boundaryless Working

A report by Brivo in partnership with WORKTECH Academy



Content

1 Executive summary 3

2 What is boundaryless security? 4

3 Why is hybrid working a challenge to security boundaries? 6

4 What can be done to protect boundaries? 10

5 The way forward 15

1 Executive Summary

This report sets out the case for addressing one of the unforeseen consequences of the rise of flexible working – the rise of boundaryless security.

When everyone worked every day in an office building, the world of access and security was much simpler. Now, as patterns of work evolve, the boundaries of the organization have been extended across a vast and complex digital ecosystem of work, requiring a new approach to emerging threats to company data, people and information. A boundaryless organization is the opposite of a bureaucracy with numerous barriers and divisions. In contrast, the organization without boundaries offers interaction and networking among professionals inside and outside the organization. The organizational model is fluid and highly adaptive.

In this paper, we look at what boundaries of work have shifted, how and why they are impacting company security, and what organizations can do about it in an age of boundaryless working. We outline a framework for addressing key issues based on three "E"s: equipment, education and experience. We also explore the benefits of cloud-based access control technologies not just in relation to securing company boundaries but in attracting talent and improving the employee experience.

The report draws heavily on interviews with three leading workplace security experts and on data drawn from Brivo's 2023 Top Security Trends Report.

This is Brivo's second whitepaper with Worktech Academy, the global future-of-work research organization. In our first report, Integrating Control: Access and Security in the Age of Hybrid Working, we made the case that if companies are going to successfully implement hybrid working models, this strategy needs to be aligned with and supported by digital systems and infrastructure, starting with cloud-based security and access to the office building. We identified four different typologies for companies at different stages of their journey to integrating digital systems with hybrid adoption.

This new whitepaper takes this story forward, delving more deeply into the implications for the security of working anywhere-anytime and proposing solutions to safeguard company assets when both cyber and in-person threats are on the rise.

If companies are going to successfully implement hybrid working models, they need to be aligned with and supported by digital systems and infrastructure, starting with cloud-based security

Boundaries of work have shifted impacting company security

2 What is Boundaryless Security?

Just as the boundaries of work have been extended by the rise of flexible working, so have the boundaries of security and access control. As a result, companies now face a security threat that is bigger and more complex than ever before.

When everyone worked in the same office at the same time, security was simpler. Companies could have a security perimeter in place to protect their employees and their assets, all housed within one place. However, in the new world of work where people are working more flexibly from home or an unspecified third location, often without their employer's explicit knowledge or oversight, security becomes a more complex issue.

In the new world of work where people are working more flexibly from home or an unspecified third location- security becomes a more complex issue

Put simply, the boundaries of working have shifted. There are no longer set times or places where people are working, as hybrid or remote teams work from different time zones, countries, offices and spaces. Furthermore, as work has entered the home in a big way, the boundaries between an employee and their work equipment have become blurred. Your work smartphone and laptop might be used for watching TV or left lying around for a family member to use.

In all likelihood, people working from home will also have other people connecting to their network and accessing the internet simultaneously, meaning that the security of your company could be compromised not only by an employee but also by their family or housemates.

This, coupled with the fact that security attacks and cybersecurity breaches have increased in the past few years, suggests that the security threat companies face has never been more significant. Moreover, security breaches are becoming more costly for companies. According to Forbes, the average price of a security breach increased by 10% to $4.24 million, and this average cost rises further when the security breach is brought about by hybrid working.

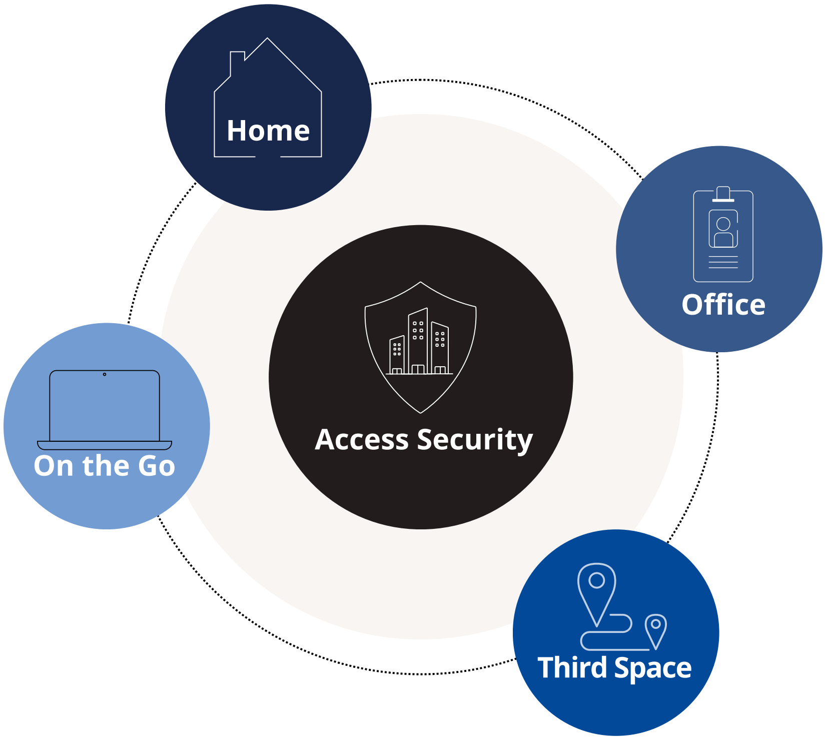
Companies cannot afford to be complacent when it comes to their security - they must now ask themselves how they can ensure the same level of security that they had pre-pandemic in the new hybrid world of work. This all comes back to the idea of identity – how do you know that the person trying to access your network from a strange location at a strange time of the night is your employee just trying to do their work and not a security threat?

How do you know that the person trying to access your network from a strange location at a strange time of the night is your employee just trying to do their work?

Having a security system that is appropriate for hybrid working and takes into account the complexities of the modern world of work is the answer, making access control and management one of the most crucial parts of your security defense.

Cloud-based access security can allow people the flexibility to work wherever and whenever suits them without compromising the safety of their organization or its data. It, therefore, sits at the nexus of the modern way of working. In this sense, it is the enabler of hybrid working, not only allowing you to control access to your buildings remotely but also allowing you to monitor your buildings and gather data on them to make you more efficient and more responsive.

> Cloud-based access security allows people the flexibility to work remotely without risking the safety of their organization or its data.



This framework illustrates the position of access security in the wider network of the hybrid employee – it not only affects the employee's experience within the office but also provides the gateway and sets the example for security at home, on the go or in a third space. Having a high-functioning access security system, such as a mobile access or biometric system, allows employees to work flexibly - with staff able to work from home with the knowledge that they are able to come into the office when it suits them with the minimum of fuss.

How well employees understand the access security system, the potential threats to the company, and the protocol around security also sets the standards for working on the go; well-informed and well-adjusted employees will be able to replicate security-related behaviors they understand and treat with seriousness.

3 Why is Hybrid Working a Challenge to Security Boundaries?

As the boundaries between home and work life become blurred, companies are examining the security implications and unforeseen consequences of the hybrid work model. This section explores the emerging threats and internal challenges.

Hybrid working has shifted the boundaries of company security, and many organizations are only just starting to wake up to the myriad of security issues and complications that this switch has brought with it.

Work-life As Home-life

When the pandemic started, companies made the switch to remote working very quickly, panic-buying laptops and other IT equipment without reflecting on their level of security. Most companies were far more interested in business continuity than security – and this lack of perspective was risky.

Additionally, many companies neglected to re-educate their employees about the new risks and problems that hybrid working brings to their security system. This includes employees not knowing whether they could use public Wi-Fi when out at a coffee shop or rely on cellular data while out-and-about, or whether they could help other staff get access to the office through the new remote-monitored access security system.

With staff working from home or third spaces, often without their employer knowing, and coming into the office more sporadically, there are more threats to company security from sources that were previously not even considered by companies. As Head of Credo Consulting, security expert Antoinette King states that in the new world of work, there is 'no division between personal and work-life engagement, creating a risk far greater than in the controlled environment we had before. The digital footprint of the individual is now part of the company's risk.'

> The digital footprint of the individual is now part of the company's risk
>
> -Antoinette King, Credo Cyber Consulting

If you are working from home and your family members are also using the same network, your company data is then intermingling with their online activity, meaning that the boundaries between your online life at home and at work are well and truly blurred. As a consequence of these new risks, there has been a huge rise in security breaches; companies are being targeted and experiencing both complex cyber security breaches and in-person breaches relating to tailgating and other security issues.

Tailgating was once not a serious threat to a company as security teams placed in lobbies of buildings would recognize staff or cross-check their image against their ID, meaning that it was hard for the unrecognized or unwanted to access the hub of the building. But since the pandemic, it has become a significant issue as teams were separated from the office, and not everyone will be familiar with new employees hired during the pandemic.

This has meant that someone asking to follow you into the building because they have misplaced their ID or building pass has become significantly easier to pull off, and without in-person security teams, there is no second layer of security to check in with.

Round-the-clock Access

Remote working also shifted the job market, with companies now able to access a wider talent pool and hire people from more distant locations. Whilst this was a success in terms of hiring a diversity of talent and accessing new skills, it now meant that companies experienced new problems in terms of security. Previous security systems often relied on patterns of behavior and regularity: understanding the standard model meant the system could flag something out of the ordinary.

Remote and hybrid work with new employees in different locations and on different schedules has torn this system down. No longer do people enter the office at the same time every day, making it harder to flag what is a risk and what is standard working practice. Predictability has given way to unpredictability, making old systems for security management outdated and ineffective.

> Previously, threats were often unintentional, caused by mistake or negligence, but now staff can become an intentional threat.
> -Mike Gips, Gips Insights

There have also been some unforeseen consequences from the onset of hybrid and remote working, which have had a knock-on effect on security. Companies that hired workers remotely or before they had fully adapted to the new way of working may not have created the same deep connection with their staff as they have with those they saw face-to-face before the COVID-19 pandemic. This has the potential to impact the security ecosystem of your company.

Security expert Mike Gips, head of Gips Insights, explains: 'Nowadays, companies have updated their software and have prepared themselves better, but they are also managing a period of high inflation, with the Great Resignation and tech-company lay-offs dominating the news. Previously, threats were often unintentional, caused by mistake or negligence, but now staff can become an intentional threat. People who have joined a company later on may have little connection with the company and can therefore be used to introduce ransomware, commit fraud, access data, and so on.'

Antoinette King adds a further note: 'Years ago, nobody would even put a complete org chart on their website, but with platforms like LinkedIn, it's so easy to find out who is in what role at a company and create your own org chart from this information. You can then target people for your phishing networks.'

This suggests that, as a consequence of hybrid and remote working and the recent upsurge in job insecurity, the boundaries for employee behavior have shifted as well, leading to an uptick in new security threats from internal sources.

Employee Experience

Another unintended consequence of hybrid and remote working has been the growing focus on employee experience, with people re-evaluating their priorities and what they want from the office after the pandemic. Companies have found themselves focused on improving workplace experience to tempt people back into the office and increase talent attraction and retention.

Consequently, smooth access to buildings has taken on a new priority; companies want staff and visitors to access the office easily and quickly and for their experience of returning or visiting the office to be frustration-free. For new employees who may have never been to the office before, having a seamless entry is an even more crucial step designed to make them feel welcome. However, it offers new challenges as people need to be issued credentials for remote access without the safety of the building being compromised.

As a result, the traditional boundaries around access control and what it means for companies have also expanded – access control has gone from a technical security issue to a key enabler of a positive employee experience and has therefore taken on a new priority. It is now a convenience issue that HR, employee experience and property management teams have all become invested in. This has introduced new challenges for access security companies, who now have to meet new needs that were previously not on their radar.

Integration Confusion

Furthermore, as a consequence of the great rush to digital working in the pandemic, the move to the cloud has been accelerated, with many companies taking great steps towards adopting a cloud-based system for their security and their data storage. This has helped companies access their data and monitor their security and access control remotely, allowing them to gather even more data and information about their internal workings and security.

This move has been incredibly positive on the whole, but with companies adopting the software-as-a-service (SaaS) model, there has been a blurring of the boundaries around who is responsible for the safety of the data and information stored on the cloud between the organization and the service provider. Antoinette King acknowledges that 'knowing and understanding where the service provider's responsibility stops is crucial. It is not always the case that the provider is responsible for the security of data on the cloud; even with an Office 365 set-up, you pay for what you get, and therefore, you need to know what options you have and what the risks are".

Boundaries in terms of responsibility and risk have been blurred by the move to the cloud, and companies may miss the importance of a fully integrated security system that can ensure the security of their building and their online presence.

Hybrid working has altered the boundaries of not only where and when people work but also the boundaries around people's behavior, which can affect a network and those departments in the company which has an interest in security and access control. These seismic shifts have had a significant impact on the industry as well as how companies manage their security and access control needs. As a consequence, new practices have begun to emerge.

4 What Can be Done to Protect New Work Boundaries?

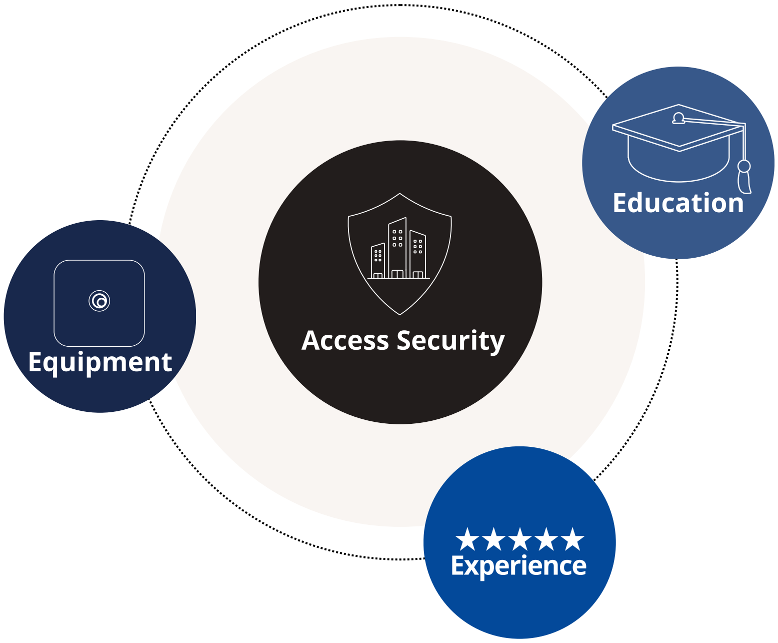
Despite the scale of the challenge, there are a number of ways in which companies can take steps to safeguard their security systems – summed up by the three "E"s - education, equipment and experience.

Given all this upheaval and all the new challenges that companies face, it can be hard for organizations to know where to start when overhauling their security to make it relevant and effective within the new world of work.

However, there are a number of steps that companies can take when it comes to ensuring their security and understanding the new boundaries of their security system. These steps can be summed up as the three "E"s – equipment, education and experience.

Despite the scale of the challenge, companies can take steps to safeguard security through three areas:

- Education
- Equipment
- Experience



Equipment

The technology a company utilizes and how this is integrated into its buildings and infrastructure is the foundation of hybrid or remote-friendly security systems. It is this equipment or technology that allows hybrid working to thrive and be convenient for employees and employers alike.

New cutting-edge technology, including biometric scanners that can assess eyes, veins and faces, and secure someone's identity from this information, can offer a seamless entrance into the office as well as secure the safety of a building.

Equipment
The technology a company utilizes and how this is integrated into its buildings and infrastructure is the foundation of hybrid or remote-friendly security systems.

Whilst there has been some hesitancy from some companies about adopting this technology, those that have adopted these state-of-the-art systems have witnessed other benefits. Lee Odess, CEO of Access Control Executive Brief, notes that biometric scanning can offer increased safety features to a building whereby the police or fire brigade is able to access biometric information and identify people quickly and easily in the case of an emergency. Narratives such as these highlight the added benefits of biometric systems and the extra levels of safety and security that they can offer.

Interest in biometrics is also increasing. Brivo's 2023 Top Security Trends Report highlights that more than 60% of the people who answered its survey are considering adding biometrics to get into their buildings in the next three years.

Double authentication and multi-factor authentication are also popular solutions and can help create a zero-trust environment where everyone is subject to the same level of scrutiny. Using credentials on your mobile phone to get access to a building is also often a worthwhile choice in a hybrid working environment, as many companies are pivoting to a mobile-first approach to workplace experience.

People are less likely to forget their phone or lend their phone to someone else, given its essential role in running our lives, which can reduce the possibility of complications on arrival at the office or tailgating. Furthermore, credentials can be stored conveniently in an Apple or Google wallet, allowing for a near-instant entry. For example, with employee badge in Apple Wallet offered by Brivo, staff can easily access their corporate spaces with just their iPhone or Apple Watch—from doors and elevators to turnstiles.

Credentials for visitors can also be authenticated remotely and issued a day in advance of their arrival, making sure that the access control system can run smoothly for everyone.

Brivo's latest 2023 trend report discusses the benefits of using a mobile-phone authentication system for access control: 44% of users found that it created lower levels of credential lending, 39% found it easier to issue and revoke credentials, 37% reported higher levels of security and 33% reported a reduced cost to run the system.

In 2022, Brivo's trend report found that 57% of respondents felt that cloud-based access control improved or could improve their overall security; in 2023, this number has increased to 66%. This suggests a growing awareness and large-scale acceptance of the benefits of a cloud-based access control system.

Having the right equipment and technology for your organization can also benefit the company by contributing to cost savings and revenue creation. Brivo's research found that using physical security data to make more intelligent and informed business decisions was the second most important aim for security professionals, with a third citing that it was important or very important.

Mike Gips notes, ‘Now that everything is moving to the cloud, companies can amass huge amounts of data about their building, access and work habits. Now companies have to think about leveraging this data and using the information they have gathered to make cost savings and increase efficiencies.’

Adopting a cloud-based access control system clearly allows businesses to gather data that helps to create a better understanding of their buildings and related outgoings in order to make targeted cost savings based on the information gathered. But it isn’t just cost saving that the right security system can support.

Increasingly, companies want to know that the people they partner with have tight security protocols. Having the right technology in place and being able to cite a state-of-the-art model can catalyze revenue generation. Antoinette King explains that ‘while security is traditionally not a revenue opportunity, companies can now hang their hats on the idea that being a very security conscious team will get more clients through the door.’

Education

Given the blurred boundaries between work and home life, as well as the increased threat of internal leaks, educating your workforce about the importance of security and the practices to put in place has never been as crucial.

Staff should be able to understand what the security protocols are, no matter what environment they are in. Regulations for staff working from home, how they should respond to sharing a network with family, how their equipment should be stored, and what this equipment is or isn’t meant to be used for are crucial boundaries to set up with your employees.

It is important that they understand the threat that their families and housemates can pose to the company. It should also be made clear if staff can work from third spaces and use public Wi-Fi if they should be using a VPN to access sensitive data, or if there are other precautions for them to take whilst at work outside of the office.

‘Teaching employees about the new threat of tailgating and other in-person threats can also then be used as a metaphor for understanding more complex cyber security threats.’

Often, understanding access security in the office is the gateway to this conversation, as cyber security threats can be complicated to get your head around. It is simpler to have in-person illustrations of what an attack on the company can look like and how to respond. Teaching employees about the new threat of tailgating and other in-person threats not only helps them understand best practices in terms of access control but can also then be used as a model or metaphor for understanding more complex cyber security threats.

Employees should also understand the threat of attacks from within the company and be made aware of processes for reporting concerns or worries about the behavior of other employees with sensitive data. As the boundaries are so much more blurred than before, education is the last line of defense against any kind of security threat. Having a well-educated and responsive workforce that understands the technology and policies in place to protect them can go a long way to ensuring that security systems do their jobs.

Education
Staff should understand security protocols, no matter their environment - the office, remote or hybrid. Having a well-educated and responsive workforce that understands the technology and policies in place to protect them can go a long way to ensuring that security systems do their jobs.

Antoinette King discusses the new emphasis on education in the security field, stating that ‘the traditional controls that you would put in place for a network don’t exist anymore, and consequently companies need to be more creative about policies and procedures and device management.’

King adds: ‘Education about security needs to become much tighter – no longer something is done once a year but every month. Also, data should be collected on who the potential risks are to a company so that educational efforts can be channeled toward them. People are always the weakest link, and training is the number one way of making people aware of their responsibility.’

Antoinette King extolls the virtues of gamification in helping people learn through reward and enjoyment rather than shaming – it’s important, she explains, that people feel like they’re part of a team with shared responsibility for the security of the company.

Additionally, one of the trends highlighted in Brivo’s latest trend report was the closer connections between physical security and cyber security, with 36% of security professionals looking at integrating identity and access management systems for cyber and physical security. Being part of the same security ecosystem and needing the same kinds of attention and control from security teams, having all your identity management systems in one place to control access to offices or to the network makes sense for security teams and can help increase the overall level of security for a company.

In the future, cyber and physical security are only going to become more interconnected, but we will also see an increase in systems integration between these two areas. This means that educational efforts on both sides should feed into the general knowledge that companies and individuals have about security, guaranteeing the smooth running of the security network as a whole.

Cyber and Physical Security We will see an increase in systems integration between these two areas, and educational efforts on both sides should feed into the general knowledge that companies and individuals have about security, guaranteeing the smooth running of the security network as a whole.

Experience

Company focus on employee experience has put new pressure on companies and security contractors to make the access security system part of a seamless office experience in order to encourage staff back into the office and make the office a welcoming and worthwhile place to be.

Employees need an experience that is seamless and remote while also not compromising on safety. Imagine someone on their first day back at the office: they were hired and onboarded during COVID-19 and haven't had an in-person experience yet. They arrive at the office and are denied access; they try and contact someone to help; they don't know who to contact, and whilst eventually they are helped into the building, the experience is diluted, and the thought of returning to the office in the future is a stressful one. Experiences like these can put hybrid workers off the in-person office experience and therefore limit the creation of an upbeat, convivial atmosphere in the workplace.

In Brivo's latest survey, 84% of companies cited user experience as significantly important to the access control experience, and when asked to rank different types of access control in terms of ease of use, 51% felt that facial recognition was easiest and 22% found that tapping a smartphone would be the most convenient way of gaining access to a building.

Security expert Lee Odess argues that the rise of experience has 'highlighted how important access control is. People who have historically been bored by access control are now paying attention, as they are more aware that having better access control options means they can access their space in new ways. But in order to create this kind of value from access control services, new stakeholders must be engaged with the program, including HR departments, experience teams, IT departments and IWMS system operators.

Tenant and workplace apps are becoming more commonplace in the workplace, and access control plays a significant role in the workplace app ecosystem. Brivo's 2023 trend report found that 9% of companies surveyed were looking at integrating their access control system into a workplace app in the following year.

Having a comprehensive idea about what access control offers the employee experience - and working as a collective to communicate this to security and access control providers - can enhance the provision of access control services and the employee experience. With an eye on experience and an eye on security, access control systems for the hybrid workplace can be seamless, and the employee experience can look more like this: You arrive on your first day, your mobile credentials have been issued in advance so you scan your phone and are instantly welcomed into the building; no stress or hassle takes place, and you continue into the space to work and collaborate.

But employee experience is not just limited to staff outside the security team. Brivo's latest report found that when asked what problems cloud-based security can solve, security professionals listed solutions that would make their lives easier as well. This included the ability to do remote door management as well as instant creation and revocation of credentials. The employee experience of security teams also benefits from cloud-based security systems, giving them the ability to embrace hybrid working alongside other employees at the company.

5 The Way Forward

Cloud-based access control doesn't just support boundaryless working – it is the first element companies need to get right to improve the workplace experience and attract and retain talent.

This report has looked at the rise of boundaryless security in the age of flexible working. Growing numbers of hybrid or fully remote workers have vastly extended the security perimeter of the organization. New ways of working have created new risks to company data and safety. This has necessitated a new approach to security and access control which is responsive to this new context and can meet the different expectations of the workforce.

With new technologies, apps and sensors entering the workplace ecosystem all the time, your security and access control solutions need to be integrated effectively within the wider workplace. Consequently, the old silos and divisions between internal teams are being eroded as groups of experts in different areas of building management are brought together by new thinking about the workplace. Security is no longer a given or a sideline of the business, it is a central element of the modern workplace, and without thinking through how security systems have or have not adapted to new ways of working, companies risk leaving themselves exposed and vulnerable to both in-person and cyber threats.

Whilst there isn't a one-size-fits-all solution, the approach advocated in this paper is centered around education, equipment and experience tools in order to create a new boundaryless security ecosystem that centers on employee experience and meets the needs of new players in the security and access control field such as HR and experience teams, as well as security teams.

Access control sits at the nexus of these three critical factors, providing the starting point for investing in new equipment, functioning as the primary port-of-call for explaining security protocol to staff, and providing the very first element of the workplace experience that employees will encounter on entering the office. This makes access control the first element companies need to get right to attract and retain talent.

Companies looking to strengthen and develop their security protocols can start here by mapping out employee experience from the moment they enter the office, the levels of education around security within the company, and the type of equipment they use and its level of integration with their wider technology network. With this perspective, companies will be able to make clear and decisive choices about how to develop their security network towards one which is boundaryless - allowing employees to work from anywhere, at any time, without compromising on the safety of company data.

The growing number of hybrid or fully remote workers has vastly extended the organization's security perimeter. Security is no longer a given or a sideline of the business; it is a central element of the modern workplace

Acknowledgments

Brivo and WORKTECH Academy would like to thank the following individuals for their contribution to this paper:

Mike Gips
CEO of GIPS Insights

Antoinette King
Founder of Credo Cyber Consulting

Lee Odess
CEO of Lee Odess Consulting

About Brivo

Our mission is to protect lives, assets and facilities with the best products and services from people passionate about quality. All security is now cybersecurity because every electronic device and software system used for physical security must first meet the challenges of cybersecurity. Here, too, Brivo started early—with more than 10 years of independent cybersecurity audits. Find out more: brivo.com

Request a Consultation

Let's get started

About WORKTECH Academy

WORKTECH Academy is the world's leading online knowledge platform and member network exploring the future of work and workplace. Sharing the latest insights, research, case studies and expert interviews with its global community of high-level professionals, WORKTECH draws on its worldwide network to harvest the newest knowledge and ideas in six key areas: People, Place, Culture, Design, Technology & Innovation. In a rapidly changing world where investment decisions require hard evidence, WORKTECH Academy provides the practical tools that shape the future of work and workplace. Find out more: worktechacademy.com

brivo

WORKTECH ACADEMY