The State of ‘Security by Design’

Is Security an Afterthought in Building Design?

January 2024

Table of Contents

People Want to Be and Feel Secure

Security by design is no longer limited to specific businesses; it's now a universal trend, evolving beyond traditional exceptions.

Despite the importance of security, it was, until recently, an afterthought in building design. Rather than considering security from the very beginning, it was addressed later. This meant costly retrofit efforts such as installing cameras to cover places with no natural surveillance, adding barriers such as planters where needed, and even adding security guard patrols. While we have learned to put thought into many other aspects of building design, such as heat, air conditioning, light, and elevators, security has not always been considered in the same way.

There are exceptions. Some buildings have an obvious security need, such as a bank or a jewelry store. But security by design has not been universal. Thankfully, this is a design trend that is changing.

Today's best practice is to plan for and integrate security from the very beginning, to be "Secure by design". This means laying out building blueprints to enhance security, and adding security features, during the design stage. Similar to the way heating and lighting are built into design for comfort, security is now built into the design for safety.

Anecdotally, we hear mixed reports about how well security by design principles are used in the field. There's often stories of how security is "patched in" after a build, rather than built in from the start. So are these principles really in place today? Or do they remain merely ambitions?

With this research, we wanted to find out if security was a priority for Architecture, Engineering and Construction (AEC) practitioners today, and if this was reflected in practice. How much time and money is being spent fixing problems post-build, and what does that mean for those designing, creating and building new structures?

Executive Summary

Our research has uncovered a disconnect between what architects and building engineers say about integrated security, and what it looks like in practice. This may be the case since security has only become a top priority in the last decade for those structures that do not obviously require security such as financial institutions, healthcare facilities, and other critical mission types of buildings.

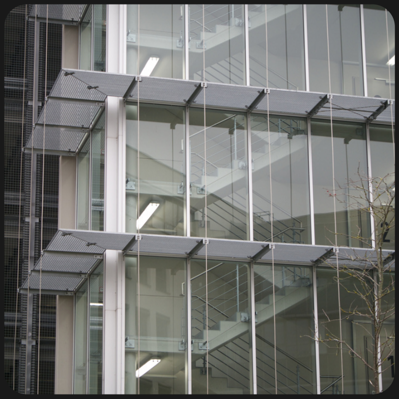
The good news is that the industry is heading in the right direction—it understands its customers’ priorities and is working towards meeting their increased security demands. But it can’t get by on attitude alone. Fully integrating best practices and getting security right the first time is the only way to fix this.

Increasingly, practitioners are adding integrated security into their processes. For at least the last decade, the demand for integrated security has increasingly become a part of client briefs. Security is, according to the AEC practitioners we spoke to, a top three priority in building design, just behind sustainability and safety.

This is reflected in the cost and time being added to projects to try and get security right. While it varies, some security costs added post-build, are as high as 20% of a project’s budget, and add a week or more to construction time.

And yet, despite the high priority given to security, the changes in processes, and the time and money associated with it, there are still clear issues in execution. In some cases, delays and costs will build up while security problems are “patched in” post-build. Initially, these costs may not seem significant when compared to the total cost of a project, but they represent far bigger issues. Delays in a building being ready can lead to frustration, a breakdown in client relations, and trigger contractual obligations for compensation as well as lawsuits.

When it comes to security, there is a clear ambition and desire for it not to be an afterthought in building design, but in practice there is an opportunity for more improvement.



Discover the hidden costs of post-construction security management in the AEC industry.

Dive into our findings revealing how firms allocate significant time, with 23% spending up to two weeks annually on post-build security fixes, shedding light on crucial challenges faced in the realm of building security.

Methodology

The survey, meticulously executed by the independent research company Coleman Parkes, involved 800 decision-makers deeply entrenched in the realms of architectural or engineering processes. Spanning the period from September to October 2023, this comprehensive data collection effort aimed to glean valuable insights. The participant pool was strategically diversified across regions, featuring 350 respondents from the U.S., 250 from the UK, and 200 from the DACH region (Germany, Austria, and Switzerland). This diverse and geographically representative sample enhances the robustness and applicability of the findings presented in this report.

#	Questions
1.	Is Security an afterthought in building design?
2.	Does your organization have a process for integrating security into the project design stage?
3.	Do you see physical security as part of the design process?
4.	Is security typically part of a customer brief?
5.	Have you seen increased or decreased demand for security integration over the past decade?
6.	What are the most common problems related to the installation of physical security systems?

Security is Becoming a Top Priority in Building Design

We conducted a survey among architects and building engineers to assess the current priorities in building design, compared with those from a decade ago. Looking back, what were the prevailing priorities in building design ten years ago, and how do they stack up against today's priorities?

TOP PRIORITIES IN BUILDING DESIGN

BEFORE*		TODAY
Safety	1	Sustainability
Materials used	2	Safety
Materials used	3	Security

*A Decade Ago

A decade ago, the top three priorities for building design were safety, materials used, and reliability, with security absent from the top three. Today, the landscape has shifted, with sustainability, safety, and security ranking as the top three priorities.

The increasing emphasis on sustainability aligns with expectations, driven by over a decade of education on adopting environmentally friendly practices. Client demands and designer recommendations reflect this shift.

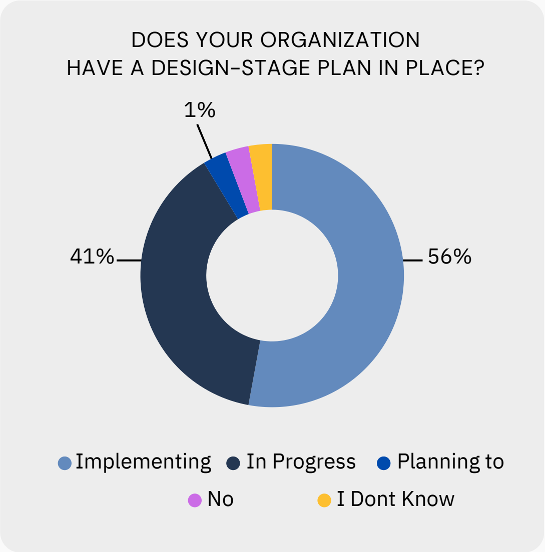
Regulations targeting carbon emissions and poor environmental sustainability further underscore the need to stay ahead of evolving rules.

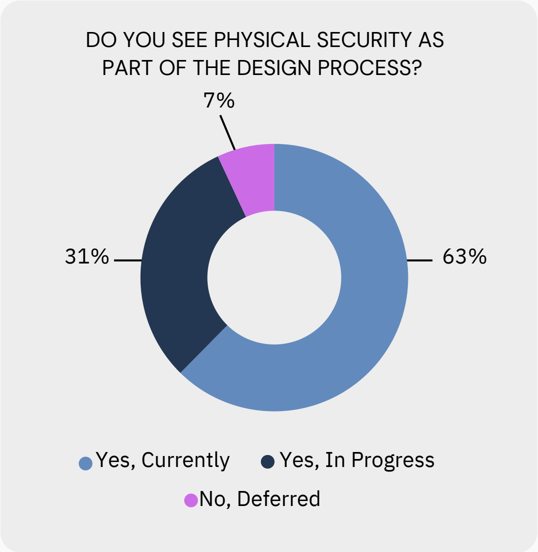
While Europe and the UK have embraced this trend more than the US, the shift towards sustainability was well underway in Switzerland a decade ago.

Security has not received the same level of attention and education within the AEC community. However, compared to ten years ago, there is now a greater awareness of the need for secure buildings, emphasizing the importance of integrating security from the outset rather than treating it as an "added extra." Security presently ranks third, following sustainability and safety, the latter remaining a steadfast top priority.

> There has been a big push in the industry to make sustainability a key consideration, and it has worked—it's now part of the design of buildings from the very start, and clients demand it. Security is different. Clients tend to only have specific demands when it's a very important part of a project, but it is absolutely something they want.

Design-Stage Strategic Security Integration: Is Your Organization Prepared?





Survey Results

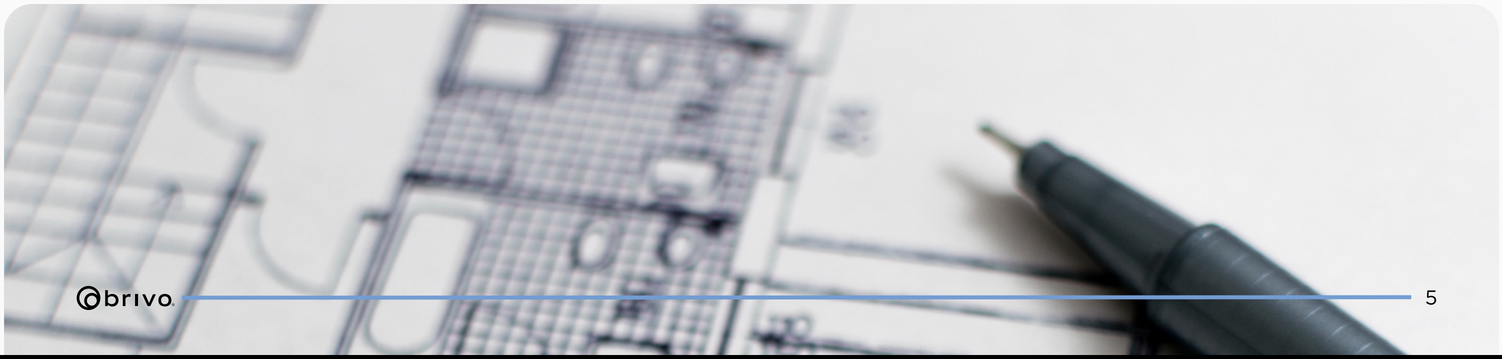
When questioned about having a comprehensive process for integrating physical security during the design stage, architects and building engineers respond positively. Currently, 56% have an established security integration process, with 41% actively with a plan in place. A minimal percentage either lacks a security integration plan or has no intentions to initiate one.

On Insights on Security Integration Attitudes: A majority (62%) acknowledge physical security as an integral part of the current design process, with 30% envisioning its integration in the future. Only 7% perceive it as an add-on for later consideration.

Furthermore, a striking 98% of those not currently emphasizing physical security in the design process anticipate a shift within the next five years. This underscores a growing industry inclination towards adopting "security-by-design," despite varying degrees of current implementation progress.

56% Have a security integration process

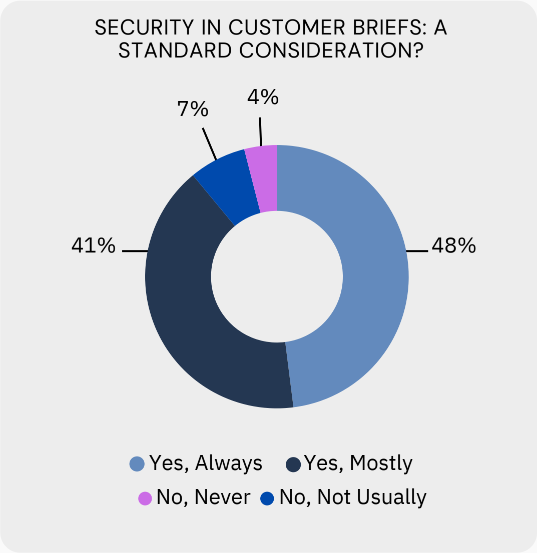
41% Actively have a plan in place

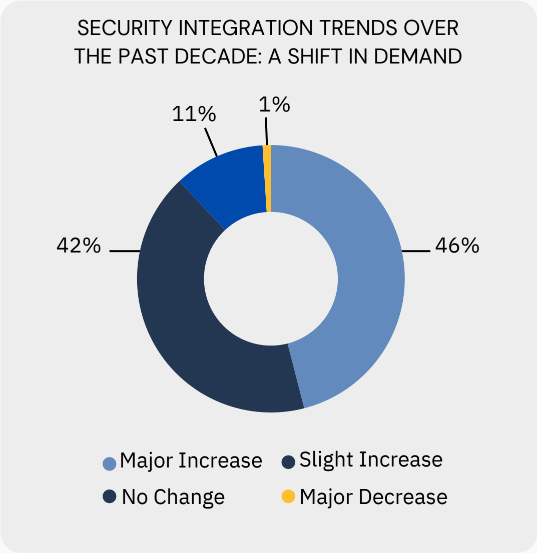


Customer Centricity and The Push for Security

Another way to measure the prominence of integrated physical security today is to examine how much is spent on it and how often it appears in customer briefs.

Do Clients Prioritize Security Enough to Include It in Their Requirements?


SECURITY IN CUSTOMER BRIEFS: A STANDARD CONSIDERATION?


SECURITY INTEGRATION TRENDS OVER THE PAST DECADE: A SHIFT IN DEMAND

Survey Results

The majority of customer briefs, as reported by 89% of respondents, incorporate security demands, with 48% emphasizing its regular and consistent inclusion.

Notably, even among the 4% who do not typically receive security requirements in a brief, three-quarters still incorporate integrated security into their proposals. In the United States, the demand for security slightly surpasses that of the UK or DACH (Germany, Austria, and Switzerland), with 95% of US respondents reporting this requirement. These regional differences suggest varying needs or awareness levels regarding the importance of integrating physical security into architectural designs.

Aligned with the increased emphasis on security in AEC design, 88% of respondents acknowledge a rise in customer demand for security integration, with 46% describing it as significant. This trend is more pronounced in the US, where 91% report an increased demand.

Impact of Not Integrating Security in the Design Phase on Project Resources

- Adds an average of 11 days to a project
- Accounts for 13% of total project cost, a substantial investment
- For 28% of respondents, costs could reach as high as 20%

Customer Commitment

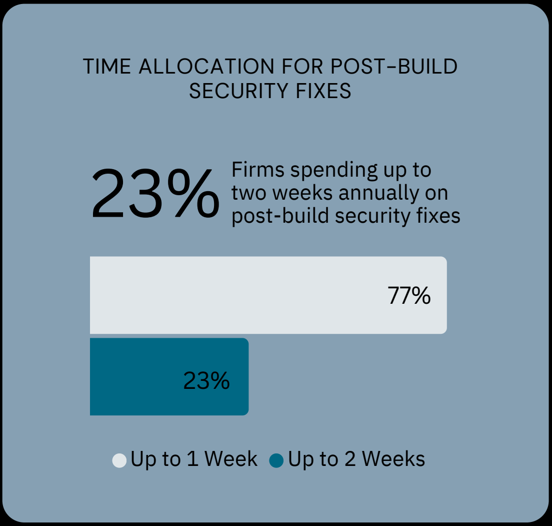
Customers not only prioritize security in briefs but are also willing to allocate significant portions of budgets towards it.

Are We Getting Physical Security Integration Right?

A significant shift is observed among AEC practitioners, with a vast majority either integrating physical security from the project's outset or working toward this goal. The prevailing trend is that most project briefs now explicitly require physical security integration, challenging the notion of security as an afterthought in building design. However, the critical question remains: Are the outcomes aligning with these aspirations?

Following construction, AEC stakeholders bear the responsibility of addressing emerging issues, including security flaws. In such cases, the burden falls on the designer, the responsible construction firm, or a collaboration of both to rectify the issues.

The time allocated to service calls for post-build security problems can result in project delays, potentially triggering contractual clauses and financial damages. Clients may also consider terminating contracts if project milestones are not met by the agreed deadlines.



TIME ALLOCATION FOR POST-BUILD SECURITY FIXES

23% Firms spending up to two weeks annually on post-build security fixes

For AEC firms still managing security post-build, an average of at least seven days annually is dedicated to addressing issues. Notably, 23% of respondents report spending up to two weeks on such post-build security fixes.

Practitioners express concerns about the inconsistency in integrating security during the design phase, leading to substantial time and financial investments in rectifying issues long after the initial design.

Challenges in Embracing Security by Design

Exploring Hurdles Faced by AEC Community

Within the AEC community, not only practitioners but the entire industry expresses its concerns about the challenges encountered in incorporating "security by design." An exploration into the root causes of this issue unveils a multifaceted landscape.

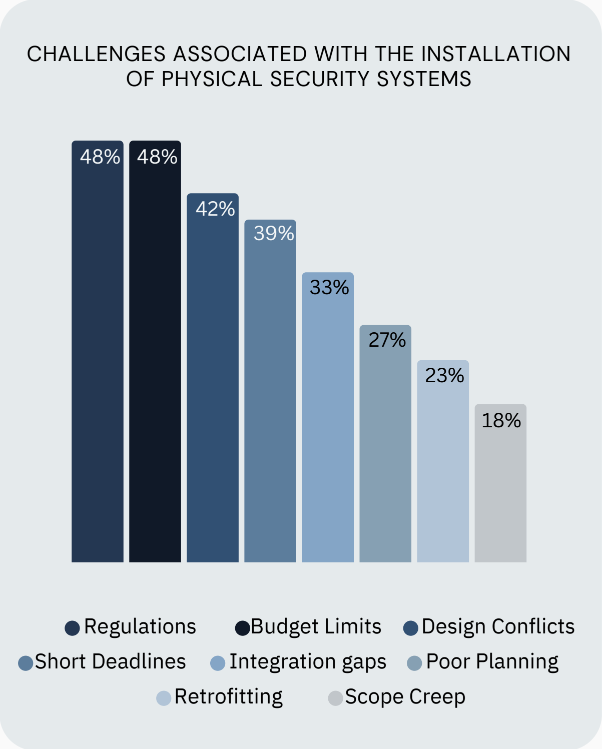
Key Challenges

Survey participants highlighted the challenges posed by changing regulations and codes, along with budget constraints—both resonating strongly at 48%. Additionally, 39% reported dealing with tight timelines, closely linked to the increasing focus on security over the past decade. This combination of challenges offers insights into the complex landscape AEC practitioners navigate as they deal with the intersection of regulatory shifts, financial constraints, and the evolving significance of security considerations in their projects.

Surprising Finding

Certainly, the most compelling finding is that one-third identified a significant problem: the absence of security integration planning. This is surprising given that many assert it's a standard practice to include security planning right from the start in the design phase.

What are the most common problems related to the installation of physical security systems?



Despite the industry's expressed commitment to making security a fundamental part of design, visible challenges persist in the integration of physical security in building design.

The current reality falls short of industry aspirations, highlighting an ongoing process of change. However, it also indicates that the industry has not yet reached the desired point of arrival crucially needed by its clientele.

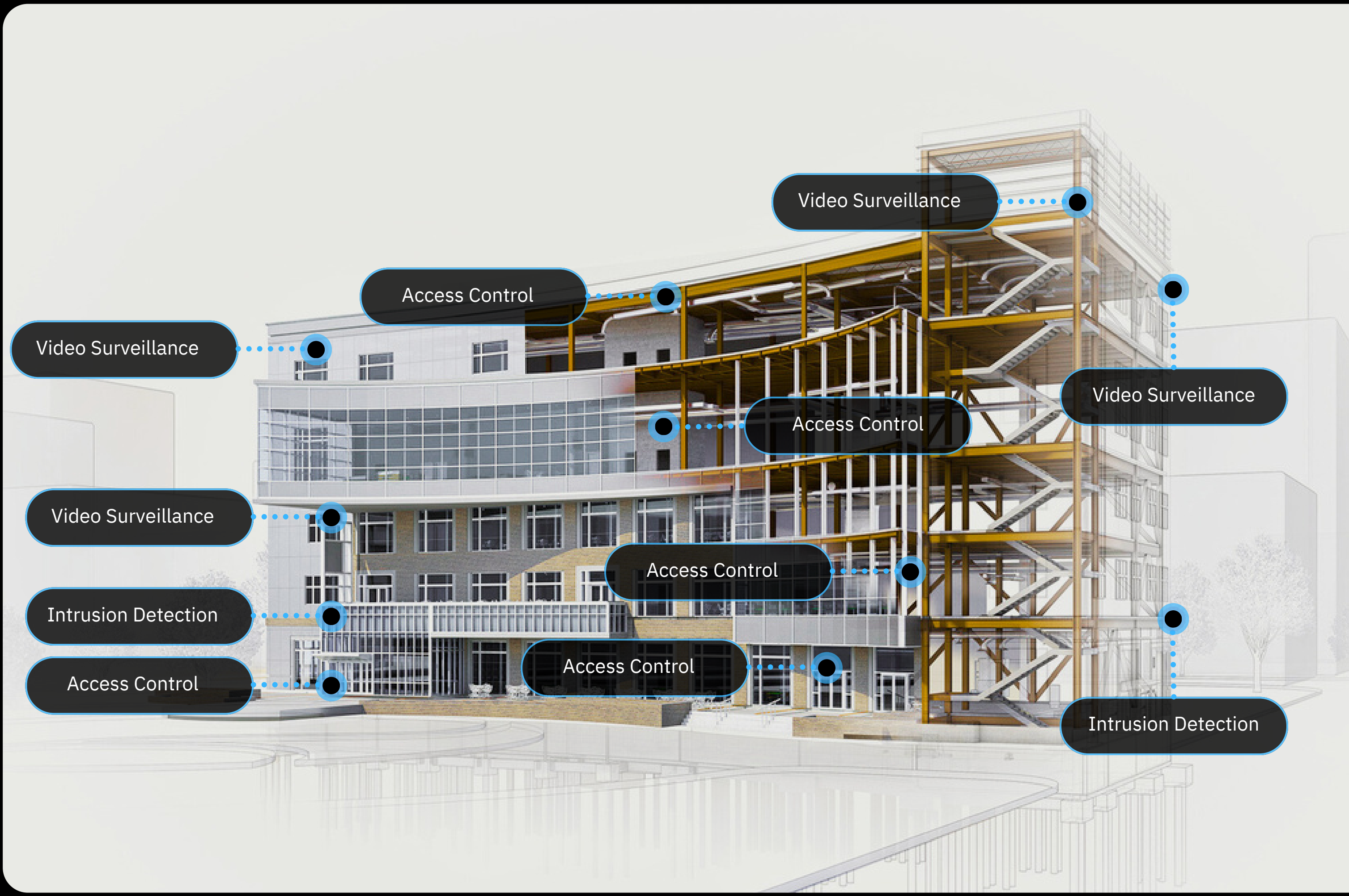
This insightful analysis unravels the intricacies of challenges faced by AEC practitioners in implementing "security by design," shedding light on areas that demand attention and strategic solutions.

Conclusion & Best Practices

This report highlights a genuine recognition of the imperative to incorporate physical security into building design, treating it akin to essential utilities like heating and lighting. Client demands for such integration are well understood, and practitioners are actively responding to this growing need.

While there's positive momentum and evident shifts in processes to meet demand, execution is trailing. The substantial time and financial investments post-build, coupled with potential consequences from delays, pose significant challenges.

A call to action is apparent for AEC practitioners to enhance the integration of security at the design stage. Acknowledging the issue is the first step, but the industry must now take concrete actions, both individually and collectively, to address this critical need.



Empowering AEC Practitioners

Industry-Wide Best Practices: Collective and Individual Approaches

01 **Training and certification**

Courses such as those that are CPTED (Crime Prevention Through Environmental Design) accredited can give practitioners a grounding in best practice. Having specialists with the right knowledge and retaining certification every three years through continuous training development will put any building design business in a great position to limit any problems.

02 **Join security by design specialist networks**

Organizations such as the ICA (International CPTED Association) are a great way to network and share knowledge, creating a better understanding of how security principles can be applied.

03 **Work with technology providers**

Providers of access control, CCTV, and other security technologies offer more than just hardware and software—they can also offer advice on how their technology is best applied and how it can be most effective.

04 **Examine design briefs closely**

Customers want security integrated into design and practitioners want to offer it, but there is always a risk of a different understanding of what this means. By making the integration of security an ongoing conversation through the design process, there is far less risk of overrunning projects and additional costs.

05 **Customer education**

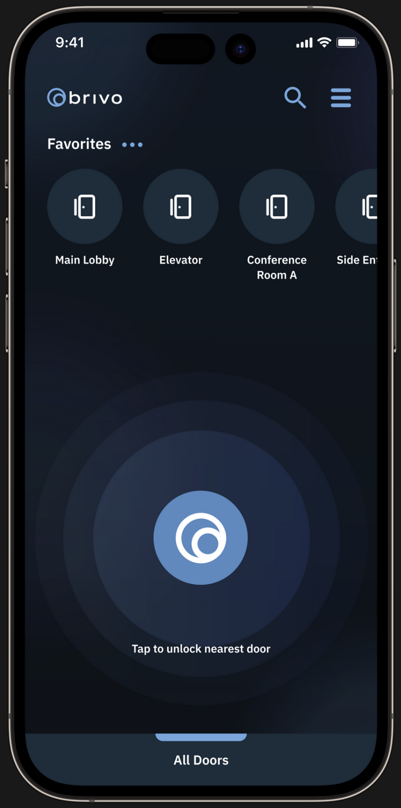
Customers may not fully appreciate the importance of integrated security and see it as something that can be patched in later. Making sure they understand just how crucial this is can help avoid problems down the line.

06 **Better processes**

Many practitioners already have a process for integrating security into design, but our results show there is room for improvement. Closely examining these processes, and post-mortems of projects where issues have arisen, can help to make these processes better. Those who are yet to implement these processes should use their networks and industry organizations to better understand the potential pitfalls they face.

Let Brivo Help

- ✓ Cloud-native solutions
- ✓ Data and auditability
- ✓ SOC2 certification
- ✓ Centrally managed access management
- ✓ Integration to video
- ✓ Compliance with new and emerging rules
- ✓ Automatic software updates
- ✓ Unlimited scale – Not restricted by location
- ✓ Remote management of all facilities



ABOUT BRIVO

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, protecting over 600M+ SQ.FT of real estate across 60+ countries. Learn more at **www.Brivo.com**

Find out more Brivo AEC solutions at

visit brivo.com