ISJ INTERNATIONAL SECURITY JOURNAL

ASSA ABLOY

Wireless Access Control Report 2025

6th biennial edition

12 years researching the future of digital access

Introduction

We are delighted to welcome you to the 2025 Wireless Access Control Report, which explores key findings from an extensive market survey carried out by International Security Journal in partnership with ASSA ABLOY Opening Solutions EMEIA.

Access control continues to be one of the most rapidly expanding areas of the global security industry. This comprehensive report offers insights into the demand for wireless access control solutions – options that are not only secure and convenient, but provide a reliable means of managing access, surpassing the capabilities of many traditional systems.

As you progress through the findings within this report, you will gain an understanding of developing perspectives within the sector. Industry voices highlight the importance of wireless technologies, particularly in the context of access management. Key statistics illustrate how we are embracing mobile-first approaches to access control, recognising that such solutions not only enhance flexibility but introduce additional layers of value. Mobile access, in particular, is gaining substantial momentum, reflecting a shift in how security is actually being deployed today.

One of the most encouraging findings this year is the recognition of security as a vital business function. No longer is it regarded as a cost centre, but instead, a driver of enterprise value. Security professionals are empowered to make decisions that not only safeguard people, assets and data but contribute to wider business objectives – which include improved efficiency and return on investment.

The report also sheds light on how regulatory changes across the EMEIA region and beyond – paired with a need to build sustainable, future-proof operations – are influencing the adoption of new technologies. While this trend signals positive momentum for the industry as a whole, it also underscores the necessity for organisations to adapt to a complex and unpredictable world.

The security landscape continues to be shaped by a range of threats across physical and digital realms. In response, teams must continue to evaluate the suitability of each solution they consider, understanding that a one-size-fits-all approach is not realistic. Findings in the report reinforce the importance of carefully selecting tech that aligns with goals, risk profiles and environmental contexts.

This year's report reflects not only the accelerating pace of technological innovation in the wireless access control space, but also the redefinition of security as a business function. As organisations navigate a rapidly changing threat landscape, their ability to implement intelligent, cost-effective solutions will be critical to achieving sustainable growth and resilience.

"Findings within the Wireless Access Control Survey 2025 demonstrate that digital access control is now the industry standard. Convenience, security and reliability continue to drive extensive adoption, but businesses must continue to navigate a complex reality; challenges around integration, trust and cost are a factor, even as organisations embrace mobile-first strategies and cloud-based models. What's striking, however, is the shift in mindset: Security leaders are no longer just chasing functionality. Today, industry leaders continue to think about long-term resilience, sustainability and alignment with evolving legislation and standards."

James Thorpe
Editor, International Security Journal

ISJ

About **International Security Journal**

ISJ is the digital and print platform for senior security professionals, manufacturers, solutions providers and industry professionals. ISJ is partnered with experts and top brands to deliver updates and valuable insights, with each monthly issue of the magazine featuring exclusive interviews and thought-leadership articles from security leaders occupying vital positions across the sector.

ASSA ABLOY

About **ASSA ABLOY**

The ASSA ABLOY Group is the global leader in access solutions. Every day, we help billions of people experience a more open world. ASSA ABLOY Opening Solutions leads the development within door openings and products for access solutions and homes, businesses and institutions. Our offering includes doors, door and window hardware, locks, access control and services.

Supported by ASSA ABLOY

ISJ INTERNATIONAL SECURITY JOURNAL

Contents

Executive Summary

The 2025 Wireless Access Control Report paints a picture of a maturing market where digital and mobile solutions are the norm.

With strong momentum in wireless adoption, sustainability, and cloud services, the focus now turns to increasingly intelligent integrations and to demonstrating ROI to cement access control's role in a new generation of smart, secure, and efficient buildings.

Access control is evolving rapidly – and 2025 marks a moment of significant transition. This report captures the perspectives of almost 500 security, access, IT, and facilities management professionals, offering a snapshot of the landscape across the EMEIA region.

Wireless, mobile, and cloud-native systems are becoming the default, rather than the exception. As new technologies like biometrics begin to take hold, the role of access control is expanding – not just as a security function, but as a key enabler of convenience, compliance, sustainability, innovation, reliability, and operational efficiency.

Wireless access rises again, and is now often the first choice

- Digital access systems are now the norm, driven by convenience, security and reliability
- 42% of end-users now deploy wireless locks (up from 39% in 2023)

Accelerated mobile access adoption, but also growing saturation?

- Access solutions in 17% of organisations are now fully mobile (up from 5% in 2023)
- Just 19% of survey respondents see mobile as unsuitable (down from 31% in 2023)
- Only 26% now plan to adopt mobile credentials in the next two years (down from 39% in 2023)

Cloud and ACaaS continue their upward trajectory

- Access Control as a Service (ACaaS) is gaining strategic traction
- Businesses favour its reliability, cost efficiency, and reduced IT costs

Powered by affordability, biometrics becomes part of the digital access mix

- A vast majority (91%) now view biometrics as a useful access and/or authentication technology

Any concerns about the security department's lack of influence are on the wane

- The proportion of survey respondents agreeing that 'Security decisions are regularly made or influenced by "non security experts"' now 14%, significantly down from 41% in 2023
- Only 16% agreed that 'Security isn't really considered a "core business function", down from 33% in 2023

Sustainability's prioritisation grows in line with wider business strategies

- 85% consider sustainability a factor in their choice of security solution
- 27% of survey respondents list it as their top procurement priority (up from 22% in 2023)
- Forthcoming regulations, in Europe and beyond, will probably see increased focus on Environmental Product Declarations (EPDs) for access technologies

An element of uncertainty remains about synergies between physical and cybersecurity

- Large majority (84%) feel cybersecurity compliance is under control or not relevant to their situation
- Uncertainty remains among nearly half (45%) about the role access control may play in cybersecurity

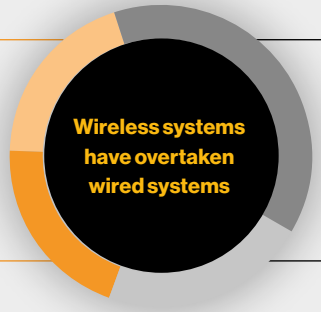
Trends in Wireless Access Control

Our 2025 Report confirms what many in the industry already realise: wireless access control is now a strategic pillar of building operations. With mobile and biometric options becoming mainstream, and sustainability driving many new decisions, access control has clearly moved beyond reliance solely on the mechanical key. We cover mobile, biometrics and sustainability later in this Report.

For security professionals, this is an era of convergence – not only between physical and digital systems, but also between departments, disciplines and objectives. Organisations which lead in access control will be those that view it not only as a security tool, but as an enabler of business-wide transformation. Integration of digital access management with other systems is critical to the creation of the holistic smart building.

Wireless access solutions are no longer experimental. With adoption climbing steadily – from 39% in 2023 to 42% in 2025 – they are now integral to modern access management strategies and workflows. For the first time in over a decade of researching and publishing this Report, wireless (fully or partly) systems have overtaken wired systems among those who manage access digitally.

Does your organisation/business already operate a digital access system?



22.32%
Yes, a combined system of wired and wireless access with access cards/tags/digital keys/smartphone

38.39%
Yes, a traditional wired system with access cards/tags/ digital keys/smartphone

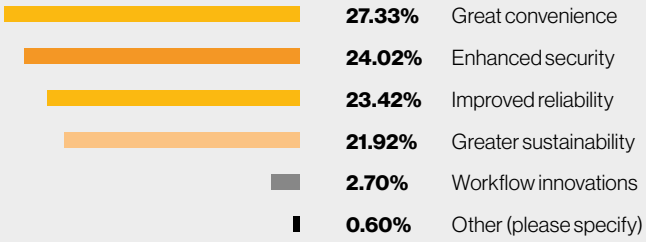
19.94%
Yes, a fully wireless access control system

19.35%
No, we do not currently have an electronic access control system

Wireless access systems provide the flexibility needed for managing everything from schools, hospitals and manufacturing plants to mixed-use buildings, multi-residential housing, and agile workspaces. Adopters cite reduced wiring, easier retrofits, and integration-readiness as a few of its key advantages. Wireless is also foundational to mobile-first environments, making it easier to support touchless entry, remote management, and real-time control.

Why do organisations continue to digitalise their access management functions? Mechanical key technology has been around for a long time. It is a proven, reliable, familiar technology for securing homes and businesses. However, end-users and security professionals see significant rewards in making the switch to digital access. The most important factor, according to survey data, is increased convenience. Viewed holistically, convenience is about much more than just small-scale savings in time and effort. When employees, contractors and temporary visitors can come-and-go with ease, operations for building and security managers are made more efficient, too. Thus, digitalising access provides a concrete ROI – something that from a strategic perspective, may be turned into a competitive advantage.

Which of the following benefits do you expect to be most important when switching to a digital access solution?



27.33%	Great convenience
24.02%	Enhanced security
23.42%	Improved reliability
21.92%	Greater sustainability
2.70%	Workflow innovations
0.60%	Other (please specify)

Digitalising access provides a concrete ROI – and may be turned into a competitive advantage

Security's growing influence within the organisation?

Another notable change between this new survey and our last Wireless Access Control Report in 2023 is the strategic position of security in relation to the rest of the business or organisation. The 2023 Report notes,

> *evidence from this year's Wireless Access Control survey confirms … that security decisions are often made by those without security experience. Over two in five (41%) respondents agreed with the statement 'security decisions are regularly made or influenced by non-security experts' while one in three (33%) said that security isn't considered a core business function within their companies. Worryingly, 30% stated that the security budget was insufficient – though this was lower than [a November 2022 report from the Security Research Institute[1]], which found that 46% of security managers/directors thought their current budget was insufficient.*

Our 2025 respondent data is strikingly different. This is especially apparent in contrasting responses to the same question asked in 2025 and 2023, about influence over security decision-making: *Which of the following statements do you agree with?*

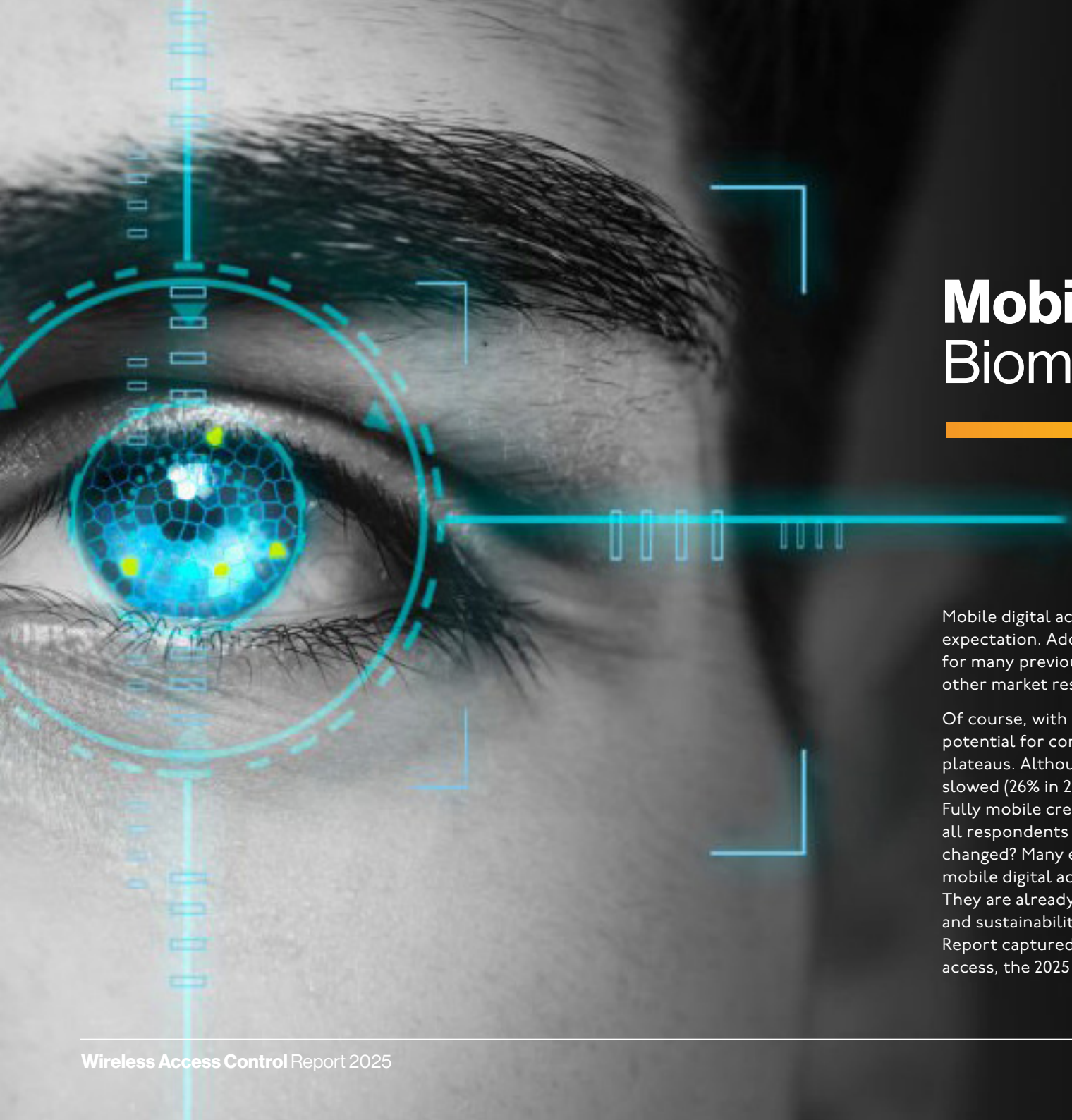
- Security isn't really considered a 'core business function': 16% agreed, down from more than a third of respondents in 2023 (33%)
- Security decisions are regularly made or influenced by 'non security experts': 14% agreed, significantly down from 41% in 2023

The latest survey, then, seems to indicate that worries about a lack of budget, or lack of strategic or 'core' positioning for security within the organisation, are no longer major concerns – or are at the very least, trending in this direction.

"The data demonstrates how organisations are increasingly treating security as a critical business function, yet fewer leaders are linking security investment to improvements across the wider business. As an industry, there is still work for us to do to ensure the security function isn't siloed. Instead, we need to drive a mindset shift to show how modern solutions like ACaaS and digital access systems enable all employees to work more effectively with less downtime and increased operational output."

Adil Abdel-Hadi
Centre Director, Aman Security Training

[1] www.perpetuityresearch.com/2022/11/11/report-launch-security-managers-lack-influence-over-the-security-budget-and-how-to-remedy-that/



Mobile and Biometric Access

Mobile digital access is no longer a novelty. Increasingly, it is an expectation. Adoption has boomed, as forecasted by research for many previous editions of this Report, as well as many other market research publications.

Of course, with deepening adoption also comes reduced potential for continued growth as market penetration naturally plateaus. Although growth in planned mobile deployments has slowed (26% in 2025 vs. 39% in 2023), the market is maturing. Fully mobile credential environments now account for 17% of all respondents – more than triple the rate seen in 2023. What's changed? Many early adopters have already transitioned: mobile digital access is for the now, not just the future plans. They are already experiencing the convenience, security and sustainability benefits of mobile access. Where the 2023 Report captured the strong momentum towards mobile digital access, the 2025 edition finds increasing market maturity.

Why choose mobile digital access?

Increasingly recognised by organisations across almost every sector and of any size, mobile brings a range of benefits:

- Streamlined access management: fewer physical credentials, instant deactivation of a lost mobile key
- More convenient user experience: faster entry, improved flexibility, using a device they already carry
- Operational agility: over-the-air permissions updates and other access management tasks can be done from anywhere

For some organisations, mobile still is not a fit. Think, for example, of some healthcare environments, pharmaceutical premises, or food preparation businesses. Yet the number of respondents who rule out mobile continues to shrink from edition to edition of this Report: just 19% of survey respondents reject mobile altogether, down from 31% in 2023.

Clearly, challenges in terms of market education remain in considering the advantages and potential drawbacks of mobile access. When asked about the obstacles, if any, to mobile adoption in their organisation, the two most popular replies were security and cost, both with 24% of respondents. Given that neither of these is necessarily true with a well-specified and -supported mobile access solution, manufacturers and system integrators still have work to do to convince everyone in the market. An opportunity to share knowledge, and therefore boost growth – in a market where around 459 million[1] smartphones subscriptions are active in Western Europe alone – is there.

[1]www.statista.com/topics/3341/smartphone-market-in-europe

Rank the following advantages in order of their importance when implementing mobile credentials.

	Average score	Final positions
Security *(unable to clone)*	**6.34**	**1**
Cost	**6.22**	**2**
Convenience	**6.16**	**3**
Security *(less likely to share with an unauthorized person or colleague)*	**5.75**	**4**
"Greener" – or more sustainable	**3.67**	**5**
Easy updating/blocking	**3.64**	**6**
Modern image	**2.46**	**7**
Contact-free solution	**1.77**	**8**

However, as organisations continue to modernise their security infrastructure, digital access systems are becoming standard, with a clear shift toward mobile credentials. Convenience and enhanced security drive adoption, despite concerns around cost, compatibility and implementation complexity. The momentum toward mobile-first access control is undeniable. It will continue, as businesses look to streamline operations and future-proof their security systems. For this generation of digital natives, the convenience benefits of mobile credentials and digital wallets are too great to ignore.

Save time with mobile key monitoring

Mobile workers can save time, cut wasted journeys, and work smarter with the CLIQ Connect mobile app by updating their CLIQ Connect keys via Bluetooth. The app transmits access authorizations and validity updates. With CLIQ Connect+, an extension to the CLIQ Connect app, non-BLE key users also have visibility on cylinder access, key schedules and the remaining validity period, freeing up time for admin staff.

Smarter, safer premises with biometric access?

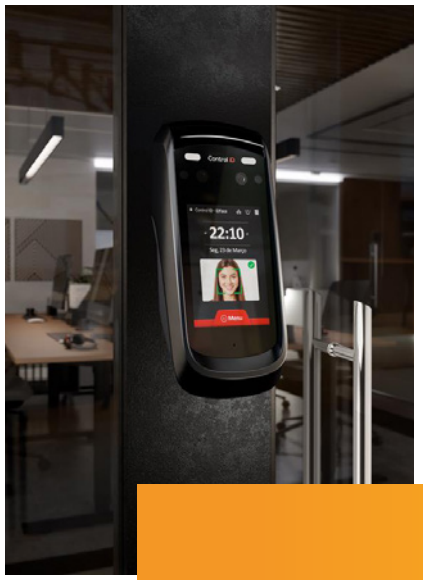
In 2025, biometric access is emerging as a serious, scalable option in physical security, not just for sensitive facilities, but increasingly for general commercial settings. Survey data shows that a vast majority (91%) now view it as a useful access and authentication technology. More than half of respondents (58%) already deploy biometrics to some extent.

Does your organisation intend to implement biometric access at any of its properties in the future?

We have implemented some biometric credentials, but predominantly continue to use physical and/or mobile credentials	**35.40%**
We are likely to implement biometric credentials within the next two years	**32.82%**
We already use biometrics as our principal access technology	**23.00%**
Biometric credentials would not be the right solution for my organisation	**8.79%**

In access control, the use of biometric technology is forecasted at 8% CAGR through 2028. The drivers for its success are easy to understand. Access systems which use biometrics, particularly facial recognition, offer tangible security and convenience benefits:

- No lost or shared credentials
- Frictionless user experience
- Streamlined entry for staff
- Easy for contractor and visitors



Biometric systems also benefit from increasing user familiarity: people are already using them to unlock smartphones and validate mobile banking. For facilities managers, biometrics reduce the administrative burden of managing cards or fobs and eliminate risk from misplaced credentials. Adoption remains cautious in some sectors due to cost and privacy concerns. But with modern platforms offering secure data handling and seamless integration, biometrics are clearly stepping into the mainstream.

"Devices like the iDFace reader from Control iD are helping reshape perceptions of biometrics as only a niche or high-end technology, due to its complexity and potential cost. This winner of the 2024 Best Biometric Product at the at the Kings Excellence Awards, it offers high-grade facial recognition performance even in darkness, and at an accessible price point."

Victório Rodrigues
International Sales Consultant, Control iD

[1] technavio.com/report/biometric-access-control-systems-market-industry-analysis

Sustainability and digital access

Across every sector of the economy, organisations are under growing pressure to align their operations with environmental goals. Whether driven by Environment, Social, Governance (ESG) targets, regulations, or customer expectations, sustainability has moved from a talking point to a board-level imperative. Businesses are rethinking infrastructure, energy use, and procurement decisions through the lens of environmental impact.

While measuring a clear return on investment for sustainability initiatives can be complex, especially when benefits are long-term or indirect, these efforts often lead to meaningful value creation over time. Within the built environment, digital access and security systems are helping close this knowledge gap by enabling smarter building management, reducing waste, and cutting energy consumption in quantifiable ways. Additionally, benefits may be financial as well as ethical and environmental. For example, the uplift in sale or rental valuations of certified 'green buildings' can be significant. According to property consultants JLL, 'buildings with better sustainability credentials are achieving markedly higher capital values and rents'. They estimate uplifts of 20.6% and 11.6%, respectively, in one analysis of BREEAM-certified premises for the UK office sector.

[1] www.jll.co.uk/en/newsroom/environmentally-sustainable-real-estate-attracts-higher-prices

Energy efficient access with mobile keys

Devices for the SMARTair straight-out-of-the-box digital access solution are powered by standard batteries for improved energy efficiency. The entire range works with the Openow® mobile app, eliminating the need for plastic cards, increasing user convenience and reducing carbon footprint.

From supporting role to strategic driver?

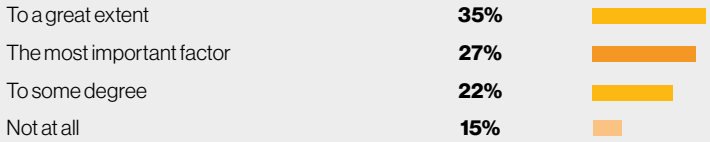
According to the International Energy Agency (IEA), buildings consume approximately 30% of global energy[1]. Increasingly, end-users and security professionals are identifying concrete ways in which digital access can help to reduce unnecessary usage. Research for this 2025 Report clearly indicates that, for many, sustainability has moved beyond being 'merely' a consideration: for 27% of respondents to our survey, it is the top factor when considering technology investments which enhance access management. Wireless systems, which reduce the need for cabling and complex infrastructure, are often seen as a 'greener' alternative.

Other signals of change in this market include:

- Growing demand for recyclable components and battery-free solutions
- Interest in solutions which support LEED, BREEAM, and other certifications
- Access management as a future-oriented driver of energy-saving automation
- Supply chain innovations which cut the embodied carbon content of devices

Within the organisation – and especially when dealing with the C-suite – demonstrating how security can align with ESG goals makes it easier to secure buy-in, especially from finance and operations leaders.

Over the next five years, how much will your choice of access control technology be affected by sustainability concerns?

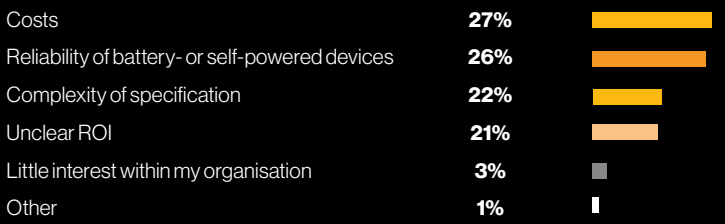


According to another survey of industry professionals, demand for green building certification is growing rapidly among decision-makers in the built environment space[2]. To meet this demand, ASSA ABLOY experts, for example, provide in-depth support for architects and developers seeking accreditation in any of six leading green certifications: BREEAM, LEED, Green Star, WELL, DGNB, HQE[3].

Electric or digital building systems require ongoing energy consumption, 24/7 and year-round for most premises. Wireless systems generally operate in a way which reduces energy consumption. Instead of an 'always on' mains electricity connection powering their lock magnets, many wireless devices only 'wake up' when presented with a credential. Energy use in operation is eliminated altogether if locks are powered by energy harvesting[4] technologies. These self-powered devices do not require batteries or any other external electricity source. Further along the product life-cycle, every building system needs maintenance. However, they don't all require the same level or frequency of visits. Less maintenance translates to fewer journeys and lower energy consumption. Again, wireless access technologies can hold a significant advantage which is recognised by respondents to the survey: cable-free operation (21%) and reduced maintenance (19%) were the top two choices from survey respondents asked how access control products should contribute to sustainability performance. However, concerns about the relationship between access and sustainability remain, notably cost, complexity and defining an ROI. For vendors, knowledge-sharing work in this area remains to be done.

[1] www.iea.org/reports/buildings
[2] www.edie.net/report-55-of-commercial-property-firms-recorded-increased-demand-for-green-buildings-amid-covid-19/
[3] www.assaabloy.com/hr/en/solutions/topics/bim-specification/bim-green-buildings/green-building-certification
[4] internationalsecurityjournal.com/security-sustainable-building-assa

What is your or your customers' biggest concern about investigating – and investing in – more sustainable access solutions?



Digital locks powered by energy harvesting technology

With the programmable key system ABLOY PULSE, kinetic energy generated by inserting the symmetrical key is harvested to power the lock's encrypted digital security. This energy source – keyholder input – is fully renewable, with no need for batteries or wires.

A growing role for Environmental Product Declarations (EPDs)

As ESG pressure grows, buyers are demanding more transparency – and Environmental Product Declarations (EPDs) hold the clearest, most holistic lens over impact. The most authoritative way to gauge the environmental impact of a product over its life-cycle is with an EPD. An EPD offers a detailed mapping of its footprint from raw material, through manufacturing, logistics and impact during use, to end-of-life recycling. Thus, product-specific EPDs help architects, specifiers, contractors, developers, green building scheme assessors and housing providers to make accurate forecasts about both embodied carbon and finished building performance.

From 2026, construction products in Europe will gradually integrate the declaration of the results from an EPD as part of the CE Marking process – and therefore, essential to sell a product or solution to the European market. EPDs fill a knowledge gap which is crucial to realising the common goal of a smarter, more sustainable built environment. Many projects already require an EPD to specify a product or solution, well ahead of the forthcoming European regulations.

> *"Digital access solutions can significantly boost building sustainability. Choosing wireless, energy-efficient systems and using EPDs helps achieve savings in both operational and embodied carbon. It's a smart step toward greener, future-ready buildings."*
>
> ***Olympia Dolla***
> ***Head of Sustainability Program EMEIA, ASSA ABLOY***

The use of EPDs has grown fast in the commercial sector, as building operators seek granular projections about future energy use. Full implementation of the revised European Performance of Buildings Directive[1], from 2028, will also enforce. disclosure of carbon footprint of products via EPDs in the residential sector. From 2030, the same regulation requires all new-builds to declare total whole-life carbon, including embodied carbon. This mandate will most likely expand to apply to renovations from 2030 and onwards.

Critically for green building specification, EPDs also contribute towards certifications such as BREEAM and LEED, increasingly sought by both developers and their tenants, for both ethical and, as detailed above, potential financial reasons. Each EPD helps stakeholders including building specifiers to make an informed and transparent choice in line with their sustainability goals.

[1] energy.ec.europa.eu/topics/energy-efficiency/energy-efficient-buildings/energy-performance-buildings-directive_en

Integration, interoperability and the cloud

Integration remains vital. However, in 2025 only 72% of survey respondents rated open architecture as 'very important' for an access solution or hardware – down from 90% in 2023. This fall suggests, tentatively, that basic integration capabilities are now merely the minimum requirement for any major investment in access and security management. Integration capability is still essential, but perhaps no longer a differentiator between solutions which an end-user may be considering. Modern access management solutions routinely support integration with door entry, video/CCTV, visitor management and HVAC, perhaps even internal payments, payroll and other business systems and software. It is open architecture and intuitive APIs/SDKs which enable such easy, seamless interoperability.

How important do you think open architecture and interoperability is when choosing or recommending a security system?

Very important	**36.25%**
Somewhat important	**36.50%**
Fairly unimportant	**16.45%**
Not important at all	**10.80%**

The benefits of integrated systems are still well recognised: they save employee time, facilitate compliance, and reduce errors by removing any need for manual double-entry in parallel systems. As has been widely noted in other market research, security and facilities professionals, including OEMs and systems integrators, are prioritising platforms that support:

- Flexible, scalable APIs and intuitive SDKs
- One interface for access, alarms, and more
- Data-driven decisions via real-time analytics

The difference with native integration

Native integration between Aperio wireless digital devices and an EAC system ensures security staff extend their control without adding workload. It does this by fully integrating new locks with the single system database. Administrators update one interface, once, without running systems in parallel or duplicating tasks. Only native integration makes new devices a seamless part of an existing system.

Cloud and ACaaS: evolving from novelty to necessity?

Across multiple business functions, in many different sectors, externally hosted systems are gradually replacing traditional, server-bound setups. Real-time control, simplified maintenance, and remote management have made cloud solutions a pragmatic choice, particularly in multi-site or hybrid work environments. Cloud adoption is often driven by the appeals of automated software patching – including security fixes – lower upfront investment, and the faster speed to get a solution up and running, improved scalability and uptime when compared with on-premise and/or self-hosted solutions. Concerns around cyber risk and data residency persist – but with the right vendor, organisations are often willing to make the trade. More than half (54%) of respondents to our survey choose cloud-based access management, either locally hosted (32%) or with third-party management (22%) on a SaaS-type model.

Within security management specifically, Access Control as a Service (ACaaS) is increasingly viewed as a strategic enabler, with real-time control, automated compliance, cost efficiency, and cyber-liability management at the forefront. According to Memoori research, the global access control market is experiencing steady growth, driven by technological advancements such as mobile access, biometrics, and IoT integration[1]. The shift towards cloud systems and the adoption of ACaaS models are central to this evolution, offering organisations enhanced scalability alongside cost efficiencies. As a consequence, the ACaaS market specifically is projected to grow from $1.34 billion in 2024 (€1.18 bn.) to $3.06 billion by 2029 (€2.71 bn.), with a CAGR of 17.9%[2].

Convergence of cloud control and easy integration

The ABLOY CUMULUS access platform, winner of multiple access innovation awards including ISJ Leaders in Security, was built API-first to simplify integration with access management, booking or workflow software solutions. The device range includes padlocks, a key deposit and swing handle ideal for applications in critical infrastructure. It also brings keyless mobile unlocking to any electric or electronic lock – from any brand – via its revolutionary CUMULUS Controller, operating reliably even where there is no smartphone signal.

[1]memoori.com/portfolio/the-physical-access-control-business-2023 [2]www.securityworldmarket.com/na/News/Themes/iam-and-access-control-technology-a-perfect-match-for-smart-buildings?

Businesses value these scalable, subscription-based models because they can reduce overhead including internal headcount, outsource compliance, and ensure prompt and/or automatic access to the latest security updates. However, lingering concerns about cybersecurity in the cloud – particularly data protection – highlight the need for trusted service providers with robust support and transparency concerning where data is stored and how it is accessed. Strikingly, only 15% of respondents to our 2025 survey say they have no concerns at all about managing security in the cloud. Conversely, 20% of respondents choose an ACaaS solution specifically because, in their judgement, it shifts liability for external cyber-attacks onto their service provider.

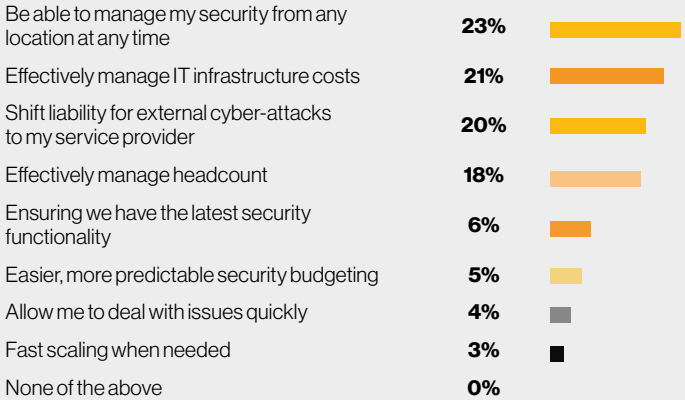
"Access Control as a Service reflects a broader convergence trend, with physical security now aligning more closely with IT, sustainability, and workplace experience strategies. ACaaS solutions have become more than just reducing CapEx, they can be used as a foundation for data-driven operations. Organisations increasingly use access data to support occupancy analytics, ESG reporting, and operational efficiency. Cloud access systems are increasingly leveraged not just by facilities managers, but by also by CIOs and ESG leads. Success in this space will depend on platforms that clearly demonstrate business value, delivering resilience, efficiency, and compliance, rather than focusing solely on traditional security functions."

Owen Kell
Senior IoT & Security Research Associate, Memoori

Smart, scalable digital access management in the cloud

ASSA ABLOY Access is designed to unify the broadest range of locks and credentials within one scalable cloud-based solution, suiting anywhere from a small business to a large housing complexes. It allows organisations to combine tags, energy-harvesting smart keys, card, PIN and mobile access, via devices including cylinders, readers, and padlocks, and manage everything from one intuitive interface.

What business goals would you hope to achieve from Access Control as a Service (ACaaS)?



Cybersecurity and compliance

The previous edition of this report covered – in some detail – key pieces of cybersecurity regulation which already, or soon will, impact digital access management. Important regulations include, but are not limited to, the following:

- Network Information Security 2 (NIS2)
- European Cyber Resilience Act
- Product Security and Telecommunications Infrastructure (PSTI) Act 2022
- European Cybersecurity Act

The vast majority of 2025 survey respondents (84%) felt they were either already compliant, or in the process of ensuring compliance, or that these regulations were not relevant to their specific situation. More worryingly, when asked directly if their organisation was prepared, 16% replied with a blunt No.

“

“Cybersecurity risk management is a significant issue for UK industry. We have seen, with the attacks against Marks & Spencer, the Co-op, Harrods and Peter Green Chilled, the fragility of UK retailers and supply chains with respect to cybersecurity risk management [...] The US, EU and Australia have enacted cybersecurity regulation that includes EU NIS 2, DORA and the Cyber Resilience Act. The US SEC enacted its cyber-rule in 2023, the NY DFS, and Australia enacted its cybersecurity act in November 2024. Cybersecurity is quickly becoming a regulated risk for companies, either directly or indirectly, requiring boards to address cybersecurity risk management or risk civil and/or criminal penalties.”

Andy Watkin-Child
Cybersecurity Expert

We predominantly focus on physical, including digital, security in these biennial reports, rather than cybersecurity. However, while there often remains a difference in job role between the cyber and physical security departments, this 'responsibility gap' is slowly closing. Having an efficient and convenient access control system is insufficient without the appropriate mechanical and digital security controls. If the digital part is insecure or flawed, the entire system is vulnerable, and the same goes for the mechanical part. In addition, combined cyber–physical attacks are on the rise, where attackers may breach a system remotely, and then exploit this vulnerability in a physical way. For example, it may involve remotely opening a vehicle, or bringing down an organisation's security system to gain physical access to a highly secure area.

Cyber attacks must be viewed as a constantly moving target, and the recent development of artificial intelligence (AI) only adds further spice to the mix. According to the UK's National CyberSecurity Centre, 'Artificial intelligence (AI) will almost certainly increase the volume and heighten the impact of cyber-attacks over the next two years[1].'

Which of the following cybersecurity certifications/government acts are you aware of?

EU Cyber Resilience Act	**41%**
EU Cybersecurity Act	**39%**
Network Information Security 2 (NIS2)	**11%**
Product Security and Telecommunications Infrastructure (PSTI) Act 2022 (UK)	**6%**
None of the above	**3%**

"In a world of emerging and evolving security threats, building users need the reassurance of reliable access control. As security converges, moving beyond physical and cyber 'siloes', the right digital access solution enables building management teams to define exactly who goes where, and when, across all their sites. Having robust, reliable, and mechanically secure access control devices isn't enough without proper cybersecurity controls in place. That's why cybersecurity compliance will soon be mandatory for any digital product sold in the EU. Staying ahead of these regulations and ensuring digital access adopters understand their importance was a key motivation this year for recording an Expert Talk video on Security.[2]"

Milivoj Simeonovski
Director & Head of Information and Cyber Security, ASSA ABLOY Opening Solutions EMEIA

For security teams, additional challenges on the cybersecurity landscape include:

- A lack of guidance from vendors and integrators
- Disconnects between IT and physical security teams
- Uncertainty around software update protocols
- Adherence to compliant data handling standards

This year's survey data shows that awareness of cyber regulation is improving – particularly around the two key European Acts. Most survey respondents (55%) acknowledge the role which access control can play in compliance at their organisation. However, many also remain unclear on whether their systems support full compliance: 45% of respondents either don't agree or are not sure if access control helps with compliance. Generally, organisations which adopt compliant systems report faster incident response and stronger collaboration with IT. Again, working closely with vendors, system integrators and other stakeholders will be crucial.

[1]www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat [2]www.assaabloy.com/group/emeia/stories/blogs/das-expert-talk-about-security

About the **2025 survey respondents**

The findings presented here are based on a survey conducted by leading industry magazine, International Security Journal. Questionnaires were submitted in April and May 2025. This survey received almost 500 responses and was open to those who work in a broad range of roles across security and facilities management, as well as IT professionals with influence over purchasing or the administration of physical access control systems.

Among job roles, almost half of respondents describe themselves as security/facility managers (49%), a far higher proportion than in any other edition of this report. The survey also gained responses from significant numbers of business owners with security oversight responsibility (8%); owners or security directors (7%); and cyber or IT professionals (4%). More than three-quarters of all respondents (76%) identified themselves as being the 'end-users' of access and security technologies – encompassing in-house security, IT, or facilities professionals such as managers, directors, or operators/administrators of physical access control systems – with the remainder classified as consultants (2%) or integrator/installer/vendor (12%), included to gain insight into the solutions they build and/or work with most regularly. Among end-user respondents, the geographical spread is typically broad. Although the largest proportion comes from the UK (64%), survey data includes a high number of responses from Germany (9%), North America (7%), and smaller but significant numbers from India, the UAE, South Africa, France, Sweden and several other European countries. End-user organisations divide evenly between small, medium-sized and large enterprises: 0–50 employees (30%); 51–250 staff (32%); 251-1,000 (25%); and more than 1,000 employees (13%).

Among a vast range of sectors represented by end-users, the largest were government/public sector (12%), industrial/manufacturing (12%), entertainment (8%), residential including multi-residences (8%), retail (6%), critical infrastructure (6%), data centres (5%), transport/logistics (5%), and hospitality (5%). A significant number of responses were also received from the following sectors: healthcare, education, commercial, and finance/banking.

Learn more

ASSA ABLOY

Make your access ready for what's ahead

We help you digitalize and future-proof your buildings with a wide range of access solutions meeting your individual needs, supporting your move from the mechanical to the digital world.
We are experts in access.

With us, you digitalize with confidence.

Experience a safer and more open world