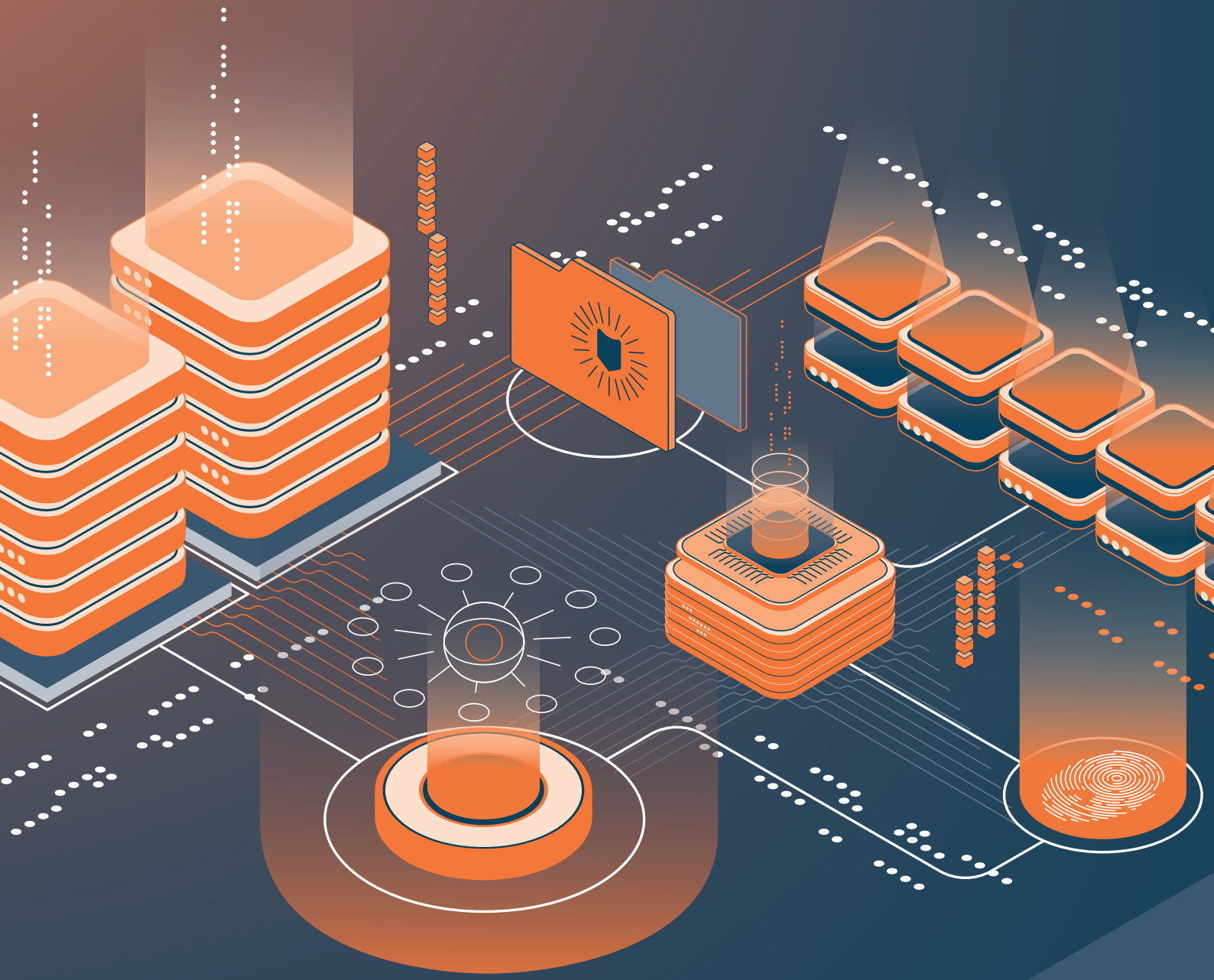


Physical Access Control Benchmark Report 2022

Global analysis of what the future of access control looks like for security and facility managers

nedap

Contents

Research Methodology:

In 2017, Nedap Security Management commissioned market research firm, The Blue Hour, to begin surveying facility and security management leaders in multinational enterprise companies. To get the full benefit of benchmarking data, digital outreach was performed by The Blue Hour before careful vetting survey participants to ensure accuracy of the target population needed.

Surveys were then performed with the target population—namely, decision makers within global enterprises. After extensive data cleaning, this report presents a sample size of 152 respondents—all of which comprise fully completed surveys.

Geographic Region

The target population was sampled across the EMEA region, including the Nordics and Scandinavia.

Industries

Respondents represented enterprise companies in the following sectors:

Aerospace & Defence
Automotive
Energy, Utilities & Resources
Financial Services
Food and Tobacco
Government & Public Services
Pharmaceuticals, Life Sciences & Chemicals
Healthcare
IT & Telecommunications
Manufacturing
Media & Publishing
Real Estate
Retail
Transportation & Logistics

Job function/Role

Respondents were identified in these specific roles:

C-level / Director / Head / Manager / Senior Manager level: Global > Local > Regional

Contracts
Corporate Security
Emergency Response
Engineers/Technicians (Mostly relevant in Middle East)
Facilities
Health & Safety (Environment/Quality)
IT/Network Security (Mostly relevant in Middle East)
Physical Security
Security
Security Governance
Security Operations
Security Services
Security Solutions
Technical Security
Workplace Management
Workplace Services

Organisational employee count

Respondents represented organizations with employee counts between 5,000 and 10,000.

Preface

How can physical access control systems add value to business?

To understand more clearly the access control challenges of multinational enterprise companies around the world, we've been benchmarking using third-party market research conducted by The Blue Hour, since 2017.

In 2020, we took our research a step further to see if we could find conclusive data on how access control could help organisations improve their business processes. In short, we wanted to learn how access control can add value to business.

Persistent change

It's clear that the relentless progression of technology is giving organisations a whole new range of ways to maximise the value of their access control systems. As IFSEC notes in its 2021 ebook, *Trends, Opportunity and Challenges in Physical Access Control:* "End users are demanding solutions that provide convenience and security in equal measure, alongside questions over integration and open standards, remote connectivity and the cloud."

But this advancement isn't without challenges. The current pace of change in technology can make it difficult for security professionals to keep up with what's on offer, what's best for their needs and how best to implement it.

A plethora of choice

With many of the big players in the access control market stepping up their product marketing and distribution channels, there is a lot of noise. In fact, Memoori Research AB, an independent analyst company focused entirely on the smart-building industry, indicates there are currently "145 established manufacturers of access control systems" (one of which is Nedap). So you can imagine the range of factors a multinational company must consider when choosing an access control system that will support its business beyond providing physical security.

The story so far, and into the future

Instead of imagining, we decided to ask. And here, we share some of the results from 150+ survey respondents to-date. We hope you'll find most helpful in your own quest for knowledge of the access control landscape – and the value it can bring to your business.

This report is structured into four parts, during which the story builds to our ultimate conclusion, providing clear numbers and beliefs on the topics of:

1. Centralised versus decentralised access control.
2. Futureproof readiness.
3. What futureproofed access control looks like.
4. What security leaders are hoping for, in an ideal world.

Executive summary

Centralised versus decentralised access control

The first part of this report reveals that fewer companies than expected have taken the step to centralise their access control, despite it offering widespread benefits. The reasons for this range from the legacy of mergers to the perceived complexity of achieving centralisation. The trend does appear to be moving towards centralisation, however, with 55% of respondents working towards centralised global access control, and many seeing great value in doing so.

Future-proofing and automation

Part two shows that futureproofing is a growing concern for many companies. Particularly as recent events such as the pandemic and the war in Ukraine have shown that threats to business continuity can emerge with little warning. Automation is a key element of futureproofing, and many of those polled stated automation as a way to optimise their authorisation process. Several also mentioned integrations, and the automations they bring, as a route to optimisation.

What future-proofed access control looks like

The third section discusses the current move towards connected or smart buildings, with access control as the hub of an ecosystem of integrated technologies. This trend is reflected by more companies now looking to integrate facilities management systems and processes with their access control systems. Biometric identification, particularly touchless technology, is also becoming more widespread.
Another significant theme for the future is mobility – both in terms of mobile workforces and people using mobile technology for access control.

What leaders are hoping for

The final part of the analysis homes in on what security and facilities managers say they'd like for the future. 'More integration possibilities' was the most popular answer by far.

The conclusion underlines that there are strong overlaps in what security and facility managers want from their systems. And access control is starting to take a central role in business operations and business continuity, with integration, automation, openness, and adaptability being major themes for the future.

Part 1: Centralised versus decentralised access control

Valuable benefits from centralisation

As IFSEC states, centralised physical access control can bring improvements in security, because you can mitigate risks more easily and ensure greater accuracy and consistency. And it can improve convenience as users can access any locations they're authorised for with one identifier.

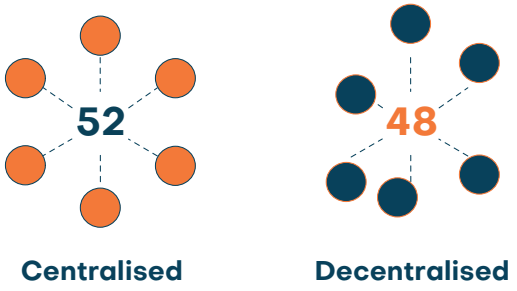
This isn't where the benefits end though. Centralisation can also lead to improvements in efficiency because administrators can manage multiple locations remotely and it takes less time to manage one system than several. And it can generate cost savings because you can take advantage of economies of scale and you only have one system to set up and maintain. When it comes to futureproofing, it's also easier to keep one centralised system up to date and adapt it to meet your future needs and risks than working with a variety of systems.

> *"Software-based applications and services are now on hand to deliver genuinely unified and centralised forms of management. The aim of all this, of course, is to improve convenience and security – equally important factors in the specification process for access control purchases."*
>
> **— IFSEC GLOBAL, Trends, Opportunities and Challenges in Physical Access Control, 2021**

Is everyone centralising?

With this in mind, we assume that centralised access control would be the preferred choice. But is that always the case? We asked security and facility management professionals around the world whether their access control is centralised or decentralised.

Is your access control centralised or decentralised?



Fewer than expected

Surprisingly, their answers were pretty much split down the middle. Some examples of why respondents say they've opted for centralised access control are:

> *"One global team has the responsibility to operate and manage the ACS for the entire organisation. This way we ensure that only trained and authorised personnel have access to the system to minimise operational mistakes that would affect the organisation. Working with critical infrastructure we are subject to strict compliance demands when it comes to ACS to our building and sites."*

> *"We have global standards and requirements that are connected to both legal and group insurance demands. We also see an economy of scale in negotiating globally and time saving than doing it in 75 sales markets, which is neither efficient nor cost effective."*

> *"The centralisation is more efficient (less costs) and more effective (better risk mitigation)."*

Why decentralised?

So, with all the benefits of centralisation, why do so many organisations still have decentralised access control systems? Sometimes, it arises organically – after a merger, for example, when existing access control systems remain in place. Or it can happen when an organisation has locations in different countries, each with their own security managers and budgets.

Sometimes, decentralisation happens simply because the scale and complexity of unifying access control internationally can feel overwhelming without the right system and support to achieve it. This may also be why some organisations end up with a hybrid of both centralised and decentralised access control.

As one respondent to our research explains:

> *"Access control was always in place in the different countries but managed locally and also sourced locally so many different solutions [were] doing the same thing."*

One respondent said they have:

> *"A hybrid mix, due to mergers and acquisitions and legacy organisations we have many fragmented site-based systems."*

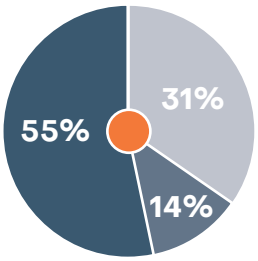
Another said their access control systems are:

> *"Mostly centralised, but in a way decentralised. Access control policy, manuals, instructions and guidelines are provided top-down and become more detailed as it reaches the individual. Document responsibility follows management out in the line organisation to ensure best knowledge is forming instructions and guidelines. Financially, we have found that company common procurement generates lowest prices and strict contract governance and follow-up ensures extra costs are controlled. Responsibility for purchase, maintenance, and service is assigned to management in respective business."*

How the future lies

This all begs the question: whatever their current situation, are organisations ultimately aiming for a truly centralised access control system? According to the security and facility managers we polled, the answer to this question is just as split:

Does your organisation aim for a truly centralised global access control system?



More than half are aiming for centralisation

55% of respondents are working towards a centralised global access control system as their ultimate goal. And many see great value in doing so, with the reasons they gave including increased security and the ability to set global security standards. Cost saving was also mentioned as a driving factor. And several respondents appreciate the ease of management that centralisation brings, stating motivations such as easier standardisation, remote configuration, better oversight and governance, uniform administration and improved data control.

One respondent said:

> *"There would be a number of advantages of moving to centralized access control. We'd have cost savings through better control of maintenance and administration plus using leverage as a large company to get better prices. Not to mention, we'd see improved security through better governance on implemented standards and the possibility of setting up operations centers."*

Some can't see a way past decentralisation

Despite there being so many clear benefits to a centralised system, 45% of the companies asked either don't plan to centralise (31%) or it feels an irrelevant option for them (14%).

So why is this? Interestingly, given that cost saving is a motivation for many companies, some respondents thought that having one centralised system would be too costly. While others were pragmatic about the realities of creating such a wholesale change in their organisation.

Support for a unified approach

Undoubtedly, international centralisation can create challenges when you're working with different cultures and legal systems and so on. But we've seen that the long-term benefits far outweigh any initial stumbling blocks, and there is lots of support available to help with unifying and standardising access control internationally.

Respondents said:

> *"Never possible within our organization, every country has their own budget and responsibility for access control. There is no global security first line operation."*

> *"Legally, a centralized access control system would be too challenging."*

> *"Centralized access control will be tough because we have a lot of leased properties with different set-ups."*

> *"We have a very complex work environment that cannot be met globally by a centralized system."*

Part 2: Futureproofing and automation

Unpredictable challenges

The covid-19 pandemic and war in Ukraine have created a sharp focus on futureproofing, highlighting that new risks to business operations – and even business continuity – can emerge with little or no warning. And it's not just health issues and wars that companies need to be prepared for. Events such as natural disasters, recession, new legislation, terrorism, cyberattacks and more can all have a dramatic impact.

Futureproofing is on the up

Compared to our previous surveys, the proportion of respondents who believe their access control system is futureproof is creeping up. Our 2017 research revealed that almost 60% of multinationals didn't (yet) consider their access control system to be futureproof. And, even in our 2020 research, 58% of those polled said they believed their current security management system wasn't fit for the future.

It's encouraging that the balance has now tipped, with more than half of those polled thinking their current access control system is futureproof. That said, 49% is still a high proportion of companies to be working with systems that may quickly become outdated and leave them at risk. Or, at the very least, at a disadvantage.

To understand the current state of play regarding futureproofing in the market, we asked:
Do you think your current access control system is futureproof?

Futureproofing is on the up

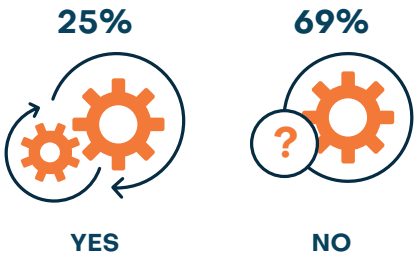
Compared to our previous surveys, the proportion of respondents who believe their access control system is futureproof is creeping up. Our 2017 research revealed that almost 60% of multinationals didn't (yet) consider their access control system to be futureproof. And, even in our 2020 research, 58% of those polled said they believed their current security management system wasn't fit for the future.

It's encouraging that the balance has now tipped, with more than half of those polled thinking their current access control system is futureproof. That said, 49% is still a high proportion of companies to be working with systems that may quickly become outdated and leave them at risk. Or, at the very least, at a disadvantage.

Automation supports futureproofing

Automation goes hand in hand with futureproofing as it enables systems to respond more efficiently to changing needs. And, in turn, enables businesses to respond better to the risks and challenges they face – as well as any opportunities that might present themselves. So we also asked respondents: the following question.

Is your authorsation model automated?



Automation for optimisation

Again, it's surprising that only 25% of respondents have an automated authorisation model, given that it's a key way to improve both security and efficiency. The benefits of automation were reflected in some of the responses to our question: **How can your authorisation process be optimised so it's ready for the future?**

Some stated automation as a key means of optimising their authorisation process And many mentioned integrations, and the automations they bring, as a way of optimising their authorisation process. In particular, several recognised that integrating their HR system with their access control would bring improvements.

> *"We could automate our authorization process using automatic workflows triggered by approvals."*

> *"More automatic controls in the software which gives badge users early information about their authorizations would optimize our process."*

> *"Integration with our HR system would give more automation possibilities."*

> *"Developing more different zones and connecting them to the HR system would help optimize our authorization process."*

> *"Implementing one central system in all our 40 countries and connecting to the HR system would put us on a path to future-proofing our authorization process."*

For us, it's clear that automation has a strong role to play in ensuring an access control system is futureproof. Whether that's by, for example, using templates to quickly apply or update authorisations; enabling pre-configured security settings to be implemented at the touch of a button; or applying rules based on integration with HR, biometric identification, building management or other systems.

Part 3: Back to (talking about) the future

Access control at the heart of smart buildings

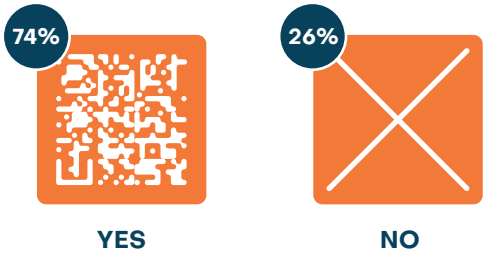
One of the key trends bringing security and facilities managers together right now is the move towards connected or smart buildings. It's creating a shift away from access control operating as a standalone security system. Instead, access control is being used as the hub of a whole ecosystem of integrated technologies. This includes security technologies such as intrusion detection and video surveillance. But also a much wider sphere of technologies that help businesses and facilities management to run more effectively and efficiently – from visitor and parking management to occupancy control, fire detection, heating, air conditioning, lighting control and more.

Both security and facilities managers can fine tune and streamline their operations based on the data and opportunities a connected ecosystem presents. And the widespread benefits of the smart-building approach include improved security, safety, sustainability and cost savings, not to mention a better experience for employees and visitors.

Increased mobility

Another key theme for the future is mobility – both in terms of workforces moving between sites and homeworking more fluidly, and people using mobile technology to an even greater degree. With this in mind, we asked our respondents their views on mobile access and QR codes and whether they believe these will overtake other access control identifiers such as cards.

Will mobile access or QR codes have the future of access control?



Strong growth in mobile access

The results reflect a strong confidence in mobile access/QR codes – something that's been gaining momentum for a while. Back in 2019, trends forecaster IHS Markit predicted that more than 120 million mobile credentials would be downloaded by end users in 2023, representing almost 15% of new credentials that year. Fast forward less than two years and the covid-19 pandemic has made mobile credentials and QR codes even more attractive thanks to their frictionless capabilities. And the opportunities they offer to add or revoke permissions and updates, and provide visitor passes remotely – all while avoiding face-to-face interactions. Another key benefit, which supports our respondents' confidence in mobile access, is convenience. Most people carry a smartphone or wearable mobile device all day every day, and so are far less likely to forget or lose it than an access card. There's also the potential to increase security by using a device's built-in security features, such as biometric identification and pin codes. And Apple's 2021 announcement that it would open up its wallet technology to app developers has created more possibilities for mobile applications in access control. Along with Android, Apple can now support both Bluetooth and NFC for access control functionality such as holding an office or hotel key card in your smartphone's wallet.

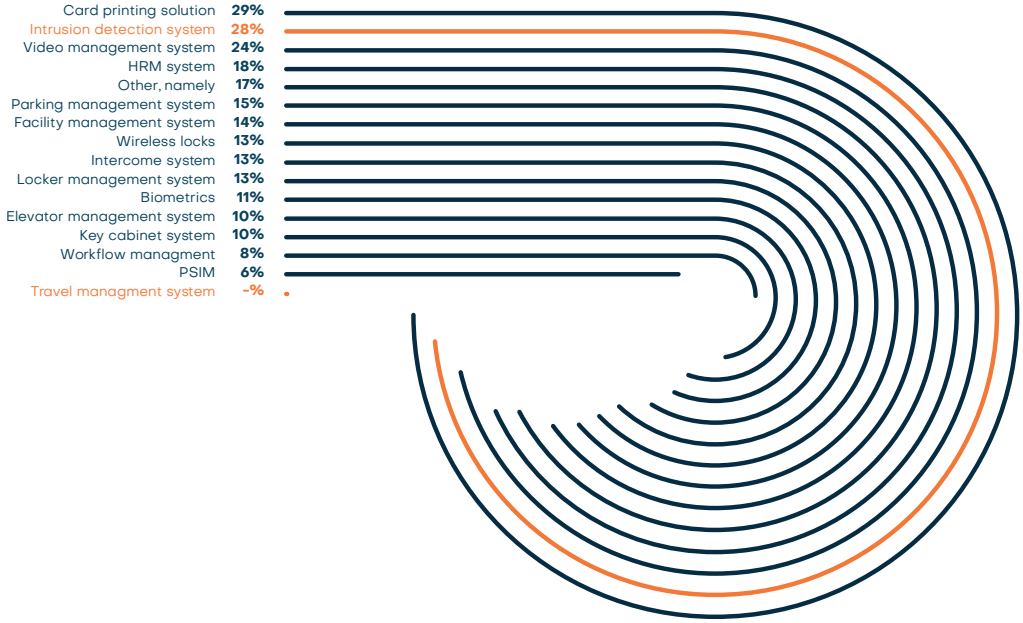
Will mobile access takeover?

With all that said, will mobile access and QR codes make more traditional credentials like cards and fobs redundant in the short or medium term? Many analysts and more than a quarter of the people we polled don't think so. Some people still have concerns around aspects such as app performance, battery life and cybersecurity on personal devices. So, although these technologies look set for exceptional growth, it's likely they'll continue to be used alongside more traditional credentials – for now.

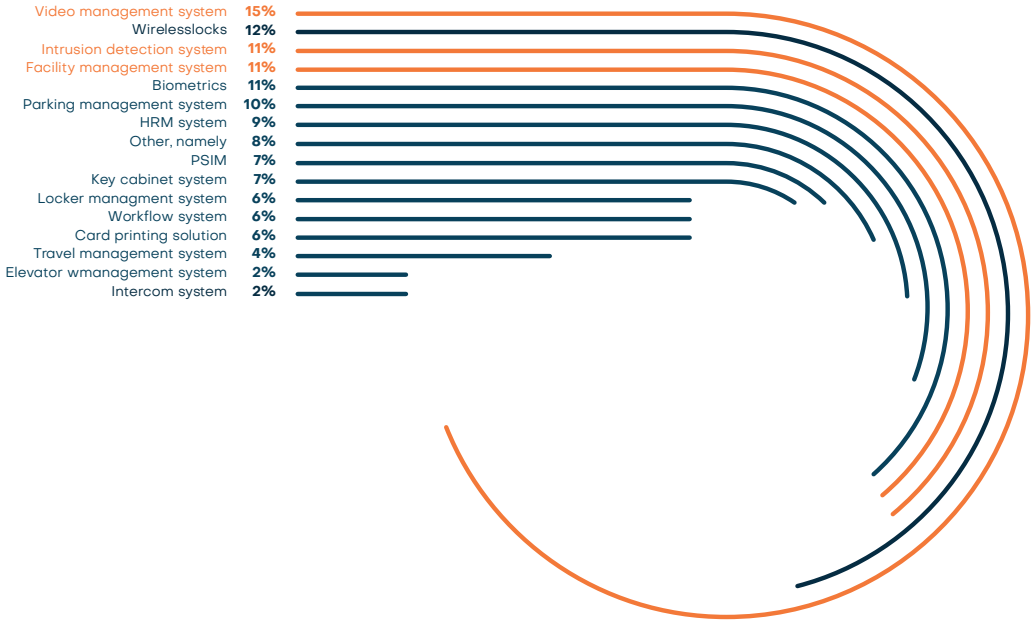
IP connectivity is transforming integrations

Of course, physical access control systems aren't only being integrated with technologies that support their operation. They're being integrated with a range of other business systems and processes too. This integration of business application services (BAS) isn't new – it's been happening for more than 20 years. What is changing is how they're connected. In the past, services were typically united by an overarching, proprietary software. But this approach can present issues in terms of costs and weaknesses. Today, systems for managing security, buildings and people can all be integrated over an IP network. What's needed for this approach to work are platforms and systems that are open to integration and standardisation. Which is perhaps why, when we asked companies which third-party systems their access control system is integrated with, there are fewer integrations than you might expect.

Which thirdparty systems are your current access control system integrated with?



Which thirdparty systems would you like to integrate with in the future?



Biometric identification becoming more widespread

What also moved up the priorities when we asked about future integrations was biometric identification. Card printing, meanwhile, went from the top spot to way down at the bottom. This could be because so many respondents already have card printing integrations it's not a high priority for the future. But it could also be because people are sensing that cards won't be used as widely in the future when there are other alternatives such as mobile access and biometrics.

Biometric identification uses people's physical characteristics, such as their face, fingerprint, iris or palm, to identify them. The benefit of this over an identifier like a card is that people can't lose or forget to carry their biometric characteristics. And it's much harder to lend them to someone else to gain unauthorised access.

In the past, biometric identification was often only used for high-security areas as it was a relatively expensive option. But costs have come down and people have become used to using biometrics on smartphones. Added to that, the covid-19 pandemic has created significant demand for touchless (frictionless) access control.

Facial recognition meets the need for touchless

Until recently, fingerprint scanning was the most popular choice thanks to its lower price point and accuracy levels. The pandemic has created a surge in popularity for facial recognition, however, with Memoori stating the market is growing at 12% year on year in its report on The Physical Security Business 2021 to 2026.

As with mobile access, the jury is out on whether biometric identification will overtake the use of cards or other physical passes for access control. What's more likely, for now, is that biometrics will be used alongside physical credentials for dual-factor authentication or as an alternative option in selected locations.

Wireless locks and remote management

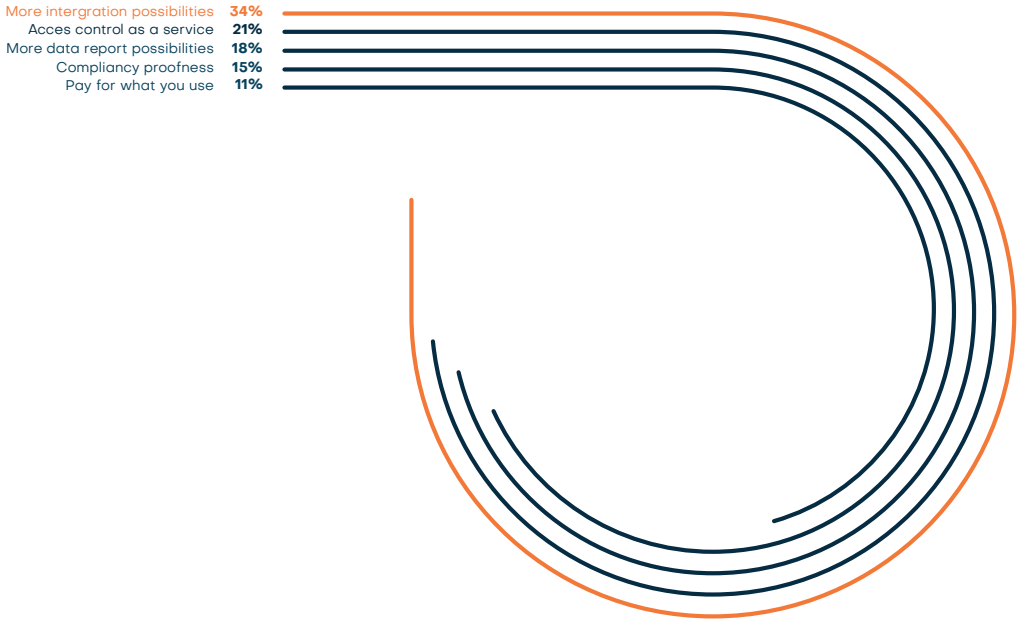
In the same way that demand has grown for touchless identifiers, we're also seeing increased demand for 'touchless' or remote management options. Which is possibly why wireless locks were a popular choice when we asked companies about future integrations. As well as being more secure, they can be reconfigured and updated remotely, without an engineer having to visit them in person.

Part 4: Playing a game of “what if”

Future wants and needs

As we come to the final section of our report, let’s look at what security and facilities managers say they would like for the future.

We asked: If you were able to redesign your access control system, what would you change?



Integrations top the wish list

‘More integration possibilities’ was by far the most popular answer (34%), and this theme continued when we asked:
If you were completely free to design your future access control system, what would it be like?

Responses citing integration as a priority included:

> *“Open source and with all the integration possibilities you could think of. Seeing as all employees have an ID card I would like to use that as an identifier in a lot of scenarios.”*

> *“Integrations with HR systems, facility management system, intrusion detection and face recognition included. Multi location with IAM connected.”*

> *“Integration into smart building concepts like use of mobile phones, biometrics instead of cards, and the ability to use identifiers (cards) for more than one facility. That‘s how our future access control system would be designed.”*

> *“Designs for a future access control system would see it centrally-managed with an access card with multiple possibilities (e.g. payments, time clock function, follow me printing etc.) and linked to our HR system.”*

Taking advantage of access control data

Third in popularity when we asked respondents about redesigning their access control system was ‘more data report possibilities’. The pandemic clearly illustrated how data collected by access control systems can be used strategically. Not just by security departments but across the organisation to both respond to a crisis and shape the future. Linked to this is ‘compliancy proofness’. With legislation increasing in all areas, access control systems can be invaluable in enforcing procedures and providing the data to prove compliance.

What else do businesses want from access control?

Other characteristics that respondents said they'd like to see in their dream physical access control system include:

- **Unobtrusiveness**

> *"The design of our future access control system would be 'Inconspicuous'" "Would love to see installation of access card readers without wiring."*

- **Easy adaptability to local needs**

> *"An ideal future would see our access |control system adapted to local needs, local requirements, and internal requirements. Where possible, it must be adapted to technological solutions that are also linked to other security measures (e.g. monitoring, alarms, etc.)."*

- **Frictionless, AI-driven control**

> *"A frictionless building system applying AI and machine learning across a wireless network."*

- **Automated authorisations**

> *"If we could design our future access control system, it would have automated allocation of mandatory access rights using ERP data records, easy application and authorisation of access requests for temporary access rights (workflows), and a function for assigning role-based access rights."*

In conclusion

United goals

We started out by seeking to discover how access control adds value to business, and therefore what the future could look like for physical access control. What's become clear in the course of this research is that there are strong overlaps in terms of what security managers and facility managers want from the systems they use.

Integration and automation lead the way

The overarching themes are integration and automation. Integration so that the systems a business uses can become greater than the sum of their parts; access control enabling other systems to operate more effectively and vice versa. And automation so that issues of efficiency and accuracy can be overcome.

Access control takes a central role

Physical access control is no longer just about protecting people and assets. It's integral to running a streamlined operation and ensuring business continuity. And it will be at heart of the move towards smart, connected buildings.

Openness is the way forward

To fulfil this future vision, systems will need to be based on software and open platforms. So they can enable easy connectivity and adaptability in a world that looks set to continue changing at an even faster pace.

We hope that we've helped you cut through some of the noise in the access control world today.

As the pace of technology continues to ramp up, we predict that the exchange of insights and best practices will become the norm. And in this spirit, we promise to continue to share our findings with you as we all move forward towards the bright future of access control.

Whatever your access control needs, our team is here to help you and your organisation in your journey. If you'd like to see where you stand in future-proofed access control, then we invite you to participate, anonymously, in our benchmark survey.

Nedap N.V. Headquarters

Parallelweg 2
7141 DC Groenlo,
The Netherlands

Info@nedapsecurity.com
+31 (0)544 471 111