

# ACCESS CONTROL 2022

## TRENDS & TECHNOLOGY

Supplement to Locksmith Ledger International, Security Business, Security Technology Executive

### THE CURRENT STATE OF AFFAIRS

The expanding adoption of PAC systems that do more than secure portals is one of the effects of the global pandemic

P. 8

#### WHAT'S INSIDE:

■ An Enterprises' Guide to Future-Proofing Their Access Control System

P. 14

■ New Standards Help Deliver a Mobile Future for Access Control P. 22

■ Even Small Access Control Jobs Translate Into Big Business P. 26

[www.LocksmithLedger.com](http://www.LocksmithLedger.com) | [www.SecurityInfoWatch.com](http://www.SecurityInfoWatch.com)

July/August 2022

**ENDEAVOR**  
BUSINESS MEDIA



RECONASENSE

#### ACCESS CONTROL WITH INTELLIGENCE

- More Control
- Early Warnings
- Fewer Tasks
- Faster Responses
- Better Decisions



See our ad on page S39



## You're the best at what you do. So are we.

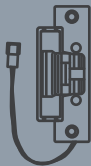
When it comes to sourcing the right parts for the job—any job—no one comes close to SECLOCK. Our team of technical service reps is unrivalled in the industry, meaning you get exactly what you need exactly when you need it, every time.

You have other things to worry about. Let us take care of the hardware.

Visit [SECLOCK.com](http://SECLOCK.com) to see how we can help.

dormakaba 

BEST 



[info@SECLOCK.com](mailto:info@SECLOCK.com)

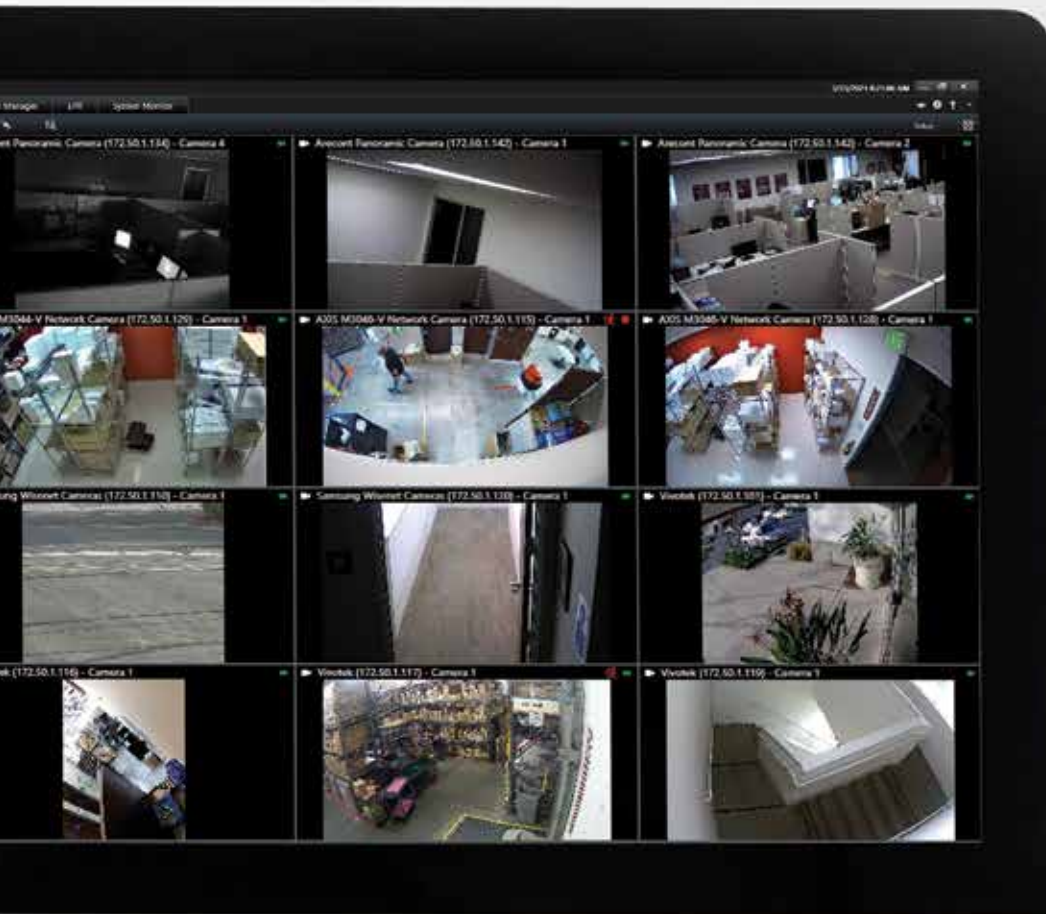
800.847.5625

# YOUR WORLD, VERIFIED.



The problem isn't security, it's awareness. Velocity Vision is the future of visual surveillance: an intelligent video management solution that delivers real-time situational awareness in an open security platform. Integrate with your existing systems, verify your environment in one pane of glass, and increase the efficiency of your security operation — get full control of your environment when and where you need it.

[go.identiv.com/velocityvision](http://go.identiv.com/velocityvision) // [sales@identiv.com](mailto:sales@identiv.com)  
+1 888.809.8880



Request information: [www.SecurityInfoWatch.com/10492079](http://www.SecurityInfoWatch.com/10492079)





Smart, scalable security solutions

Expand your business by keeping up to date with the latest updates and releases in Net2 and Paxton10.

Sign up to our free installer training today  
[www.paxton.info/5289](http://www.paxton.info/5289)



Unrivaled technical support



Nationwide installer training



5-year warranty

## Paxton Installer App

Paxton in Your Pocket – the Ultimate Installer Tool

Get instant access to all the tools you need to install Paxton products.

Request information: [www.SecurityInfoWatch.com/10215750](http://www.SecurityInfoWatch.com/10215750)



FREE download on Android or iOS



# Universal Access Control (UAC) from Immix<sup>®</sup> Guard Force

Enable RMR with Professional Access Control Monitoring



Monitor multiple disparate enterprise access control platforms from a single interface

Sync with customers' databases in real-time

Receive only the door alarms/events you want with video verification

Control any door you want

Immix<sup>®</sup> gives you the CHOICE!

**immix**

**immix** GF

One Platform. Unlimited Opportunities.

[www.ImmixProtect.com](http://www.ImmixProtect.com)

# ACCESS CONTROL 2022

## TRENDS & TECHNOLOGY

# ACCESS CONTROL 2021

## TRENDS & TECHNOLOGY

PUBLISHED BY



331 54th Ave N  
Nashville, TN 37209  
800-547-7377

Access Control – Trends & Technology 2021 is a supplement to *Locksmith Ledger*, *Security Business* and *Security Technology Executive* magazines.

### EDITORIAL

**Editorial Director** | Steve Lasky  
**Editor, Locksmith Ledger** | Will Christensen  
**Editor, Security Business** | Paul Rothman  
**Editor, Security Technology Executive** | Steve Lasky  
**Editor, SecurityInfoWatch.com** | Joel Griffin

### SALES

**Group Publisher** | Jolene Gulley-Bolton  
480-524-1119  
jgulley@endeavorb2b.com

**Northeast US & East Canada**  
**SB, STE, SecurityInfoWatch** | Janice Welch  
(224) 324-8508  
janice@securityinfowatch.com

**Midwest**  
**Locksmith Ledger, SB, STE, SecurityInfoWatch** | Brian Lowy  
(847) 454-2724  
brlowy@endeavorb2b.com

**Western US & Western Canada**  
**SB, STE, SecurityInfoWatch** | Bobbie Ferraro  
310-800-5252  
bobbie@securityinfowatch.com

**Display/classified** | Amy Stauffer  
(920) 259-4311  
astauffer@endeavorb2b.com

### PRODUCTION

**Production Manager** | Jane Pothlanski  
jpothlanski@endeavorb2b.com

**Ad Service Manager** | Carmen Seeber  
cseeber@endeavorb2b.com

**Audience Development Manager** | Delicia Poole  
dpoole@endeavorb2b.com

**Art Director** | Kayla Burger  
kburger@endeavorb2b.com

**ENDEAVOR BUSINESS MEDIA, LLC**  
**Chief Executive Officer** | Chris Ferrell  
**President** | June Griffin  
**Chief Financial Officer** | Mark Zadel  
**Chief Operations Officer** | Patrick Raines  
**Chief Administrative and Legal Officer** | Tracy Kane  
**EVP/Group Publisher—Tech** | Lester Craft  
**EVP Special Projects** | Kristine Russell  
**EVP Marketing Solutions** | Jacquie Niemiec

**Subscription Customer Service**  
Toll-Free 877-382-9187; Local 847-559-7598  
Circ.SecDealer@omeda.com

**Endeavor Reprint Services**  
reprints@endeavorb2b.com

### COVER STORY:

**8 The Current State of Physical Access Control Technology**  
– Luc Merredew

### ACCESS CONTROL

**14 An Enterprises' Guide to Future-Proofing Their Access Control System**  
– Lee Odess

### MOBILE ACCESS CONTROL

**18 The Mobile Revolution in Access Control**  
– Jeff Bransfield

**20 New Standards Help Deliver a Mobile Future for Access Control**  
– Vincent Dupart

### LOCKSMITH INSIGHTS

**26 Even Small Access Control Jobs Translate Into Big Business**  
– David Ito

### ADVANCED ACCESS

**30 AI in Security: The New Era of Access Control**  
– Shikhar Shrestha

**36 5 Reasons Why Faces Are Superior Access Control Credentials**  
– Aluisio Figueiredo

**38 Advanced Analytics The New Tool for Access Control**  
– Steve Lasky

### Advertisers' Index

Advertiser Name	Page	WebSite URL
Access Hardware Supply	S25	www.securityinfowatch.com/10722906
Altronix Corporation	S9	www.securityinfowatch.com/10212790
Banner Solutions	S33	www.securityinfowatch.com/12071932
Brivo Systems	S40	www.securityinfowatch.com/10213096
Camden Door Controls	S37	www.securityinfowatch.com/10213140
Continental Access	S35	www.securityinfowatch.com/10213301
DKS DoorKing Systems	S17	www.securityinfowatch.com/10213482
dormakaba Group	S27	www.securityinfowatch.com/12304402
Identiv	S3	www.securityinfowatch.com/10492079
Immix	S5	www.securityinfowatch.com/21152412
NAPCO Security Technologies	S7	www.securityinfowatch.com/10215125
Paxton Inc.	S4	www.securityinfowatch.com/10215750
SALTO Systems Inc	S31	www.securityinfowatch.com/10225529
Seclock	S2	www.securityinfowatch.com/10215009
Smarter Security, Inc.	S1, S39	www.securityinfowatch.com/10215136
STI-Safety Technology Int'l	S13	www.securityinfowatch.com/10214881
Trine Access	S21	www.securityinfowatch.com/10215438
UHS Hardware	S29	www.securityinfowatch.com/21143796
Viking Electronics	S11	www.securityinfowatch.com/10556843










# Access Control Made Quick & Easy

Get Hosted Accounts Online & Protected Faster than Ever with  
1<sup>st</sup> Cell-Based Access Control System Designed  
For Small & Medium Businesses



AirAccess offers a great new hosted business model for creating new commercial accounts faster and adding new security services twice as quickly, providing ACaaS, Access Control as a Service and real-time access & 24/7 emergency monitoring.

With StarLink cellular-networking, AirAccess automatically works around the customer's network or IT Dept and is flexibly wireless, from your choice of access door technology to the cloud.

-  **Easy Cell- & Cloud-Based Access Control as a Service (ACaaS)** – Flexible Options for Dealers/Integrators &/or Locksmiths @ an Affordable Flat Monthly System Rate
-  **No IT Dept or ISP/Network Changes** – Powered by StarLink Cellular, it automatically makes network-connections for you
-  **Right-Sized & Affordable for SMBs**, offices, retail, multi-tenant, gated communities &/or office parks
-  **FREE Remote App w/ Built-in Mobile Credentials**, SMS-alerts, Lockdown & door control
-  **Up to 2x RMR-Services** w/ Hosted Real-Time Access &/or 24/7/365 Emergency Monitoring option to any Central Station†
-  **Add Choice of Wireless Doors** – Wireless Panels w/ Wiegand Readers or Gate Systems/Operators or Alarm Lock Wireless PIN/Prox Trilogy Locks or Designer ArchiTech Series
-  **AirAccess Starter Kits** – Ready-to-connect hundreds of doors & users out-of-the-box; including AirAccess Cloud-Based Software w/ 5-Step Wizard – scalable for a few or unlimited users



**NAPCO Access** Ask for AirAccess at Your Security or Locking Distributor Today or call at 1.800.645.9445 • For More visit [www.AirAccess.com](http://www.AirAccess.com)

AirAccess, StarLink, Trilogy, Network are trademarks of NAPCO Security Technologies.

Request information: [www.SecurityInfoWatch.com/10215125](http://www.SecurityInfoWatch.com/10215125)



# The Current State of Physical Access Control Technology

The growing adoption of physical access control systems to monitor occupancy data is just one of the outcomes of the global pandemic

by Luc Merredew



To better understand the present state of the physical access control systems that are deployed in the market, HID Global conducted a survey of just over 1,000 respondents across a wide range of physical access control job roles and geographies. It follows similar surveys conducted by HID Global in 2020 and 2021 that likewise explored the demands and challenges of utilizing physical access control systems on a daily basis, whether significant upgrades are required, and what respondents desire from their solution to support operational practice.

While HID's 2020 State of Physical Access Control Report found that 51% of respondents believed their current system either met or exceeded their requirements, just two years later,

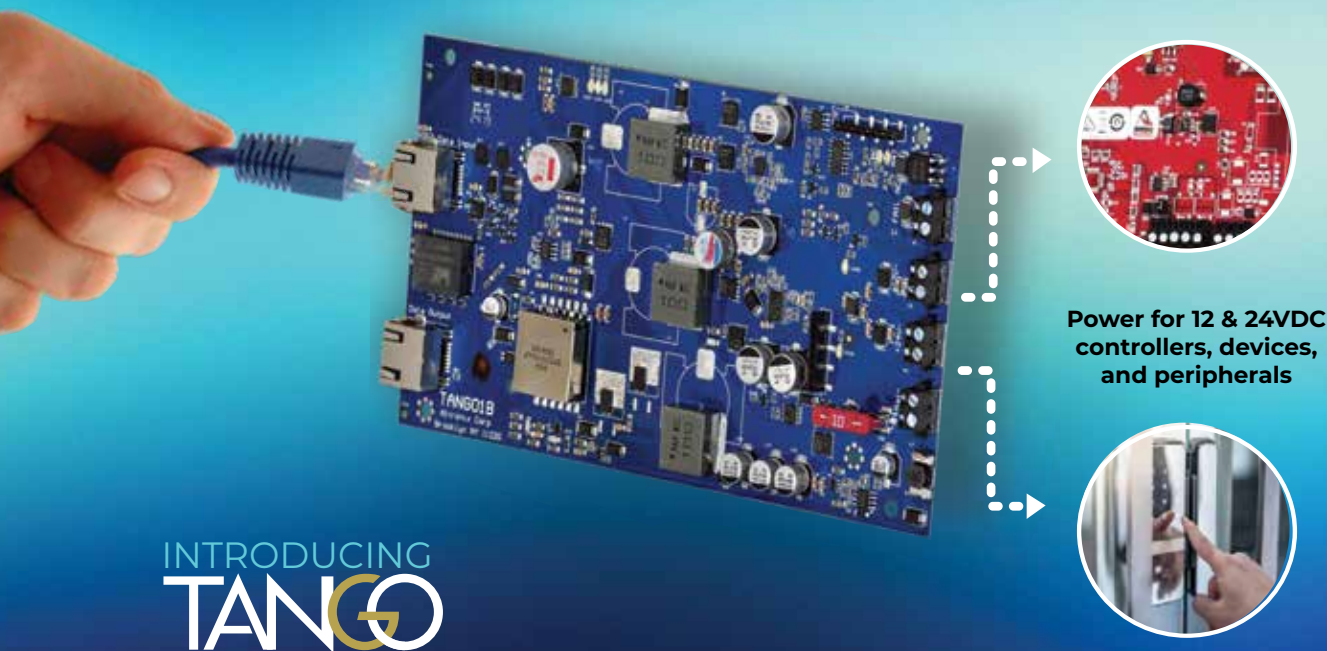
*The growing adoption of physical access control systems to monitor occupancy data is just one of the many unexpected outcomes of the global pandemic.*

*Courtesy of HID Global*



# PLUG & PLAY ACCESS POWER

4PPoE Driven Power – by ALTRONIX



INTRODUCING  
**TANGO**

**Tango power supply/chargers provide faster, safer deployments, eliminating high-voltage by utilizing 802.3bt PoE.**

- Converts PoE to 12VDC and 24VDC simultaneously
- Power your access system from a single cable, reducing costs and increasing profits
- Built-in LiFePO4 battery charger

 | Altronix®

**YOUR LEADER IN POWER SOLUTIONS**

Request information: [www.SecurityInfoWatch.com/10212790](http://www.SecurityInfoWatch.com/10212790)



Courtesy of BigStock.com

*Over a third of professionals are planning to upgrade at least one, if not all, of their access control components within the next three years.*

this figure has dropped to 41%. During this two-year period, a global pandemic has led to a significant change in fundamental organizational practices beyond what could have reasonably been predicted three years ago. Following are the most significant findings from the 2022 report.

### Traditional Credentials and Physical Badges Remain in Use

Access control credentials have undergone an evolution in recent years. Older credentials introduced in the 1980s and 1990s are unencrypted and much easier to duplicate than modern options such as Seos® and MIFARE DESFire EV3 credentials with security features such as encryption and mutual authentication that are inherently more secure. Despite this, almost a third of respondents stated they are using 125 kHz low-frequency prox, and 35% also support magnetic stripe technology. Technology such as first-generation MIFARE Classic and iCLASS is being used by 18% and 26% of organizations, respectively.

It is also unsurprising that 60% of organizations use ID badges for access control purposes—while they do provide a ready-made touchless solution. Time and attendance systems, where employees can check in and out of work for payroll and other administrative functions are being used by 50% of companies, and 49% are using parking/gate control.

Though newer technology, such as biometrics and mobile ID, is being used by fewer organizations, there is now significant uptake in the marketplace. According to the report, 32% of respondents said they were actively using mobile IDs, while another 30% are actively using biometrics technology—whether that be fingerprint, facial or iris recognition. An additional 17% of respondents cited they were planning to upgrade to

biometric access control or were already in the process of doing so, while another 19% said the same about mobile technology.

Over half (55%) of organizations are now using logical access (secure computer/network login for access to cloud and web resources)—a figure which is likely to have risen significantly during the pandemic as security and IT teams needed to ensure employees could access the necessary systems remotely, without compromising security. Many companies had to implement significant changes to their operating procedures to accommodate remote working, to prevent data leakage and cyber security vulnerabilities. The need for physical access control measures enabling hybrid work and onsite essential employees may have also played a role.

### Challenges to User Satisfaction

Improving user convenience was the challenge most cited as security professionals' top day-to-day challenge with systems, and 43% would like to make the administration of physical access control easier.

Twenty-six percent of those surveyed selected 'complying with new regulations' in their top three challenges, while 13% chose 'reducing physical touchpoints'. With one in four looking to ensure their access system is up to date with the latest regulations, and for just over one in 10 to select contactless technology as a top three day-to-day challenges, this may indicate that COVID-based practices are continuing to have an influence on security and facilities management professionals.

There is also a clear demand for more integrated systems, with 27% citing 'integrating with other enterprise systems' in their top three day-to-day challenges. With the move away from proprietary technology to open platforms, such as OSDP, organizations are able to reap the benefits of connected devices that relay information to each other to determine automated actions.

### Upgrades are a Major Issue

If only 41% of users believe their current access control system meets or exceeds their requirements, clearly there are several obstacles that remain to an upgrade process. Despite this, 38% of all respondents plan to update their physical access control system in some way in 2022. 28% of respondents were 'not sure', indicating

that decisions may depend on whether the reduction of COVID restrictions and reigniting of sector-specific economies continues.

In addition, over a third of professionals are planning to upgrade at least one, if not all, of their access control components within the next three years. While vendors continually work to make replacing systems easier than ever—particularly if staying with the same provider but upgrading to newer models—a full upgrade of readers, credentials, controllers, and/or software is not likely to be a decision made lightly. Regardless of the planning and specification processes involved, it takes installers and integrators time and money to conduct the work, resulting in potential inconvenience for staff and visitors.

Occupancy data feedback has evolved from simply knowing how many individuals are in a building or on-site for safety purposes

Software is considered the easiest to upgrade, with some providers able to integrate newer versions to older hardware devices via cloud-based updates. But it is also easier than ever to upgrade separate components of physical access control systems thanks to open software technology, such as OSDP. Technology from different manufacturers can now be integrated to work together, using open protocols rather than proprietary, closed technology, meaning that users can upgrade readers or credentials without having to upgrade both at the same time.

Traditionally, the upgrade decision-making process for a system so integral to the security of a facility or organization would likely fall directly to the security department. While major upgrade projects may require sign-off from the C-suite, much of the planning, specification and procurement process would have been undertaken by the security team, collaborating with facilities or IT where appropriate.

# BATTLE-TESTED SECURITY



When it comes to security and communication, strength matters. At Viking Electronics, we combine the industry-leading innovation of today with the tough-as-nails durability of the past.

Whether your system calls for analog or VoIP, multiple access points, or color video...

**YOU NEED A VIKING.**

 **DESIGNED  
MANUFACTURED  
& SUPPORTED**

# VIKING

**715.386.8861**  
vikingelectronics.com

Request information: [www.SecurityInfoWatch.com/10556843](http://www.SecurityInfoWatch.com/10556843)



Courtesy of Getty Images

*A move to 'touchless/contactless capabilities', which could be seen as a direct consequence of the pandemic has led to an adjustment of health and safety best practices in the workplace and multi-occupied residential buildings.*

As the industry moves away from stand-alone technology, however, the access control system – much like video surveillance – is doing far more than simply providing a barrier to entry to unauthorized individuals. Instead, as the technology and software available have evolved, access control is now integrating with HR, facilities, IT, HVAC and many more building systems.

The survey revealed that installers, integrators, consultants and vendors who deal directly with the end-user will have to balance multiple demands and departmental influences when implementing upgrades. Across the board, there appears to be some involvement from several departments in the purchasing of physical access control systems. Generally, and as one might expect for any major internal upgrade plan, the C-suite – including CISO, CSO, CIO and CTO – was most selected as having final authority. The physical security, IT and information security and facilities team were also said to have either final authority or make final recommendations on Physical Access Control Solutions (PACS) upgrades by the majority.

While very few responses cited that sustainability departments – or those professionals who have responsibility for an organization's environmental footprint (not all may have entire departments) – had the final recommendation or authority over decisions, 75% of professionals did at least have 'some influence'. 28% were even said to

be 'fully consulted' in decisions, marking a clear effort by organizations to understand how new purchases and upgrades in access control technology can have an impact on sustainable practices.

The survey also revealed the drive for physical security and cyber/IT security departments to work closer together. As physical security systems and devices have evolved into IP-based products, many are now directly attached to the organizational network. This has brought many benefits, but also challenges and concerns over potential vulnerabilities. While vendors play a key role in ensuring systems have some level of 'built-in' protection – adhering to standards such as cyber essentials or ISO 27001 – IT professionals will want to ensure that anything attached to their network is compliant and there is no risk of access from hackers, via a vulnerability in an access control reader, for instance.

Proponents of the 'convergence' of security highlight the need for a culture shift away from siloed departments with separate funding sources and strategies to one of inclusion and collaboration. Physical security hardware can be a 'gateway' for cyber-physical threats, and access control systems may therefore require both the physical and cyber departments to have oversight of the tech being used.

Despite the demand for upgrading access control, there remain several obstacles in

doing so – the most obvious of which is cost. Indeed, 38% of those asked selected this as their biggest obstacle to upgrading, while another 15% answered that there was a lack of compelling ROI and that it wasn't a business priority for the budget. Whatever the obstacles to upgrading, with 38% of respondents looking to update or upgrade some form of their access control system in 2022 alone, there is clear demand and awareness of the need to do so.

There is also a clear push towards long-term convenience, as end-users, consultants and integrators become increasingly aware of the move away from proprietary models towards open, long-term standards and solutions. Forty-nine percent of those surveyed said they would require the 'ability to add or support new tech in the future, 33% require 'integration with existing security platforms', while 28% argued for 'open-standards' based tech'.

Users are also keen to embrace innovative technology, it would appear. 43% answered 'touchless/contactless capabilities', which could be seen as a direct consequence of the pandemic which has led to an adjustment of health and safety best practices in the workplace and multi-occupied residential buildings. Despite many countries actively reducing such requirements, this number has only grown since HID Global's own State of Access Control Report in 2021 (41%).

Meanwhile, 41% required the ability to utilize mobile in a new access control system. In a separate question, where we asked respondents to select the one technology that they thought would have the greatest impact on improving physical access control, one in five selected touchless (20%) or mobile access (18%).

## Access Control's Role in Monitoring Building Occupancy

The survey also revealed how the pandemic has shifted patterns of work in organizations across the world, and how this impacts access control.

For those who have transitioned to a hybrid model of both remote and in-person work, building occupancy monitoring has become more important to ensure facilities remain as efficient as possible and to allow the c-suite to make informed decisions about building usage.

Occupancy data feedback has evolved from simply knowing how many individuals

are in a building or on-site for safety purposes, such as in the event of an evacuation or emergency, to Real-Time Location Systems (RTLS). According to the survey, 39% of organizations are able to measure both the number and location of employees and visitors on site, while 21% are unable to, or choose not to, monitor either. 34% of respondents cited they only know the number of employees and visitors on site, but not location. The final 6% only know the location of employees and visitors, but not the number – perhaps unsurprising given that most systems that are able to track location will be monitoring occupancy numbers simultaneously.

As many businesses looked to streamline their operations and save money during 2020 and 2021, those with occupancy data were able to assess whether they could ‘offload’ office space that was rarely utilized. For organizations that have transferred to a hybrid work model, such technology also allows for better planning, to ensure desk spaces are always available, but not

stretched – particularly on days that are busier than others.

Access control systems were the most popular form of method to monitor occupancy data, with 42% using them for employees and 34% for visitors. Time and attendance systems were also cited by 24% for employees and 15% for visitors, while electronic and even paper rosters remain in use – perhaps by smaller firms or for specific purposes, such as an on-site gym or leisure facilities. SMS and cellular systems were also being used by a few organizations (2%).

The growing adoption of physical access control systems to monitor occupancy data is just one of the many unexpected outcomes of the global pandemic. With a renewed focus on hygiene and safety practices and millions of people suddenly switching to remote working, the changing requirements of access control systems for security, facilities and IT teams to navigate have been more dramatic than ever before. The crossover of convenience and security has moved ever

closer, but new working practices – many of which remain despite signs of a return to ‘normality’ – have also added prominence to building efficiencies and contactless solutions. While the 2022 Physical Access Control Technology report re-surfaced many of the same themes as the 2020 study, it is in these areas that the pandemic seems to be having an enduring influence. **AC**

### About the author:

Luc Merredew is the Product Marketing Director for Physical Access Control at HID Global. He possesses over 20 years of identity management, security and life safety experience. He joined HID Global in August 2015 as its product marketing director, physical access control, and previously served in product management and marketing positions for IDENTIV, UTC Fire & Safety, Kidde plc. and Kidde-Fenwal.



## Rely on STI®



## ...to help prevent false fire alarms

### Stopper® Cover Flashes and Sounds

Universal Stopper® flat polycarbonate cover helps protect fire pull stations, without restricting legitimate operation. Ideal for use in areas where there is a risk of malicious or accidental activation.

- When lifted, cover flashes and horn sounds
- Helps stop false fire alarms
- Draws attention before alarm is activated
- Helps reduce building disruption
- Easy to install



**Safety Technology International**

Learn more at [www.sti-usa.com/sd105](http://www.sti-usa.com/sd105) or call 248-673-9898

2022

Request information: [www.SecurityInfoWatch.com/10214881](http://www.SecurityInfoWatch.com/10214881)



# An Enterprises' Guide to Future-Proofing Their Access Control System

by Lee Odess



*In reality, most legacy access control providers have been focused on today only, so in turn, so do the features and roadmap of their products.*

Courtesy of Getty Images -- Credit: Jakarm2521

**W**ithout a doubt, the technology sector has evolved. But has the access control industry grown with it?

The answer is, "it depends."

It depends on who you're talking with, what vertical they work in, their business model, and their own perceptions and experiences.

It also depends on whether or not they acknowledge that the game has changed.

## Playing a New Game

For the past 30 years, the access control industry has rested on the value proposition of keeping bad people out. There is a perception in the industry - even among "innovators" - that this value proposition does not need to change. That's led to incremental changes in architectures, legacy technologies, and the reliance on tried-and-true business strategies.

Of course, that's the value proposition. Safety and security are the foundation. And, up until recently, the traditional access control customer was not asking for anything different.

So, why change the game?

Easy. The customer changed. Their expectation wants, needs and understanding of what's possible have fundamentally shifted.

As an industry, our imperative is to provide safety and security. In that, the industry remains resolute. But looking ahead to the next 30-plus years, companies need to play a new game: one that delivers safety and security and much more.

## Vertical Software Integration Key to Unlocking Opportunity in the New Game

This shift isn't as new as it may seem. The access control industry has been moving toward a new value proposition (with a core of safety and security) since 2009 with the introduction of the iPhone. The pandemic accelerated the shift in customer expectations and the need to deliver on new vertical-specific use cases to a fever pitch - a metamorphosis this industry has not seen since the introduction of electronic access control in 1973.

This accelerated digital transformation has given way to a more software-centric industry, a savvier and more creative customer, a need for more extensive and unique enterprise solutions, and a new, customer-centric

story (aka value proposition) - one that allows for personalized experiences that not only create safety but also ease.

The pandemic also generated an influx of capital (billions of dollars) into and around the security industry which escalated this transformation even higher - faster.

Up until a couple of years ago, the high-security industry was only a cottage industry. But now, flush with the increased investments, the security industry has entered the mainstream, which can look a bit confusing through our traditional lens.

---

For the past 30 years,  
the access control  
industry has rested on  
the value proposition of  
keeping bad people out.

---

The reason? In short, verticalization. Verticalization forces industries to get very deep into the nuances and use cases it needs.

The problem for the access control industry is that, like the broader security industry, it has been working under a horizontal model where the same systems and features used for airports were also supposed to work for the enterprise, senior living or any other vertical.

Most of the acceleration in the mainstream market is happening in verticals such as proptech, multifamily or the enterprise. This is where we see new players, business models and a customer looking for something quite different from what the access control industry has been doing, saying and selling. What you see looks more like what you have seen in the HVAC, IT and lighting industry.

The customer base that is focused on a vertical model is looking for value beyond table stakes (our core value proposition of safety and security). And this is an opportunity to either lead through change or merely manage it.

## How to Future-Proof Your System

A few in the access control industry are putting action behind this and leading the way.

The rest are, to my best guess, are waiting. Or perhaps they are wishing for something else to change (so they don't have to).

No matter what, it is clear that the most successful companies will take a vertically integrated, customer-centric approach.

Which leads us to the question: How?

How does an enterprise organization create a roadmap and approach to advanced access control that is multi-faceted and future-proof?

The word future-proof is interesting and is the primary variable when thinking about how.

As I stated earlier, for over 30 years, there was a minimal need to worry about the future as the past was the only approach. Likewise, most legacy access control providers have been focused on today only, so in turn, so do the features and roadmap of their products. And that is okay because the conventional wisdom was that is all customers and dealers wanted from these systems. But as we move out of this new normal, we need to start looking at today and tomorrow, not yesterday and today.

## What Do Today and Tomorrow's Access Control Systems Look Like?

Here are three questions and eight criteria to consider when looking to future-proof your access control system. Let's break these into three categories: today, tomorrow and cost.

### Question 1: Does this access control system meet my needs for today?

Security - data, cyber, and privacy: This one is easy to understand at a high level but gets very nuanced as you dig into it, how it is applied and what it means. The simple question is, can you trust that your and your customer's data are safe? Even easier, can you trust the access control manufacturer, and can they provide you enough information to prove you should trust them?

What features do you need, and does the access control system have them? I would clarify what features you want and ensure the access control manufacturer can meet them as a standard with minimal configuration. I would also look for an access control manufacturer that can improve over time. That is the great misnomer of the access control industry. Access control systems built for yesterday see their best day on day one when they are installed. From that point forward, they degrade over time, whereas



Courtesy of BigStock.com

*The customer base that is focused on a vertical model is looking for value beyond table stakes (our core value proposition of safety and security). And this is an opportunity to either lead through change or merely manage it.*

modern access control systems get better as they age, just like an iPhone or a Tesla.

What is the usability of the access control system like? Modern companies built for today and tomorrow have an intuitive and easy-to-understand user interface. And I am not just talking about the user interface that dealers or administrators use. Modern access control systems include the end-user experience.

---

An access control system built for today and tomorrow has a solid and connected community and partners.

---

**Question 2: To what extent will the technology meet our future needs?**

Innovation Engines: I would ask the access control manufacturer to show you their modern innovations. How much

investment and effort are the manufacturer spending to improve the technology and its adoption horizontally like a “security product” and vertically to meet the needs of specific customers such as yourself? Ask for a copy of their software release notes. Then check out how many they have had and how useful they are to your business.

Flexibility: This one is hard to prove but essential to ask. Few legacy access control systems have evolved. So, make sure you ask to understand how easily their solution has evolved as the particular sector you work in, and technology has developed? For instance, do they lead with a mobile-first mentality that is fit for multifamily or the enterprise or as an extension of their card strategy that can be applied to any vertical? Then ask them to provide you with their point of view that extends out three to five years from now – is the story they are telling you to have new ideas and ways of working or is it laboring to keep up with an industry maturing at breakneck speeds? The days of proclaiming “we are a slow and conservative industry” are yesterday’s Modus Operandi.

Interoperability: This is an area where the access control industry has failed

itself more than anyone else. Our industry has decided that we will take the walled gardened with point-to-point integrations instead of focusing on standards and easy-to-implement free-flowing information. Just like the need to define the features, you desire; I would make the ease of your access control system talks with other technologies a critical path to selecting a system that meets your needs today and tomorrow. What APIs does the access control system have? More importantly, what is their philosophy on integrations, sharing of data, and portability of information?

Ecosystem: Strong interoperability typically leads to a robust ecosystem. An access control system built for today and tomorrow has a solid and connected community and partners. This strong community and partners will set you up for success for today’s needs and future ones you are not yet sure you need.

**Question 3: To what extent does the technology work within your budget?**

Configuration, Licensing, and Ongoing Costs: As access control systems move into tomorrow, they will start not only to look, feel, and sound like enterprise systems, but they will also begin to charge like enterprise systems. Getting a clear understanding of your initial and ongoing costs is critical.

We are in the early innings of this digital transformation. The good news is there are many examples outside of our industry to look to form patterns, models, and best practices. Step one, though, is acknowledging the new game. Once we can do that, we can start unpacking the impacts of that change and planning for the future. There is no better time to be in the access control industry, and there is no better time to be a customer of the access control industry. Good luck with the future. It is our industry’s opportunity to win. **AC**

**About the author:**

Lee Odess is currently the Senior Vice President of Business and Operations for Latch. A long-time physical security consultant and expert, Lee previously was the CEO and Founder of Group 337 and has served in various executive roles with Allegion, UniKey Technologies and Brivo.





# Good for the Environment Good for Everyone



## **DKS Pedestrian Protection System\***

Awareness Sensor to avoid walkers in the path of the arm.



## **Octagonal Lighted Signal Arm\***

Light the way for customers to exit easily and safely with signals and sensors.

DKS 1601 and 1602 Barrier Gate Operators are designed to run worry-free and eco-friendly for years with features like solar compatibility and 12 VDC LED low consumption Warning Signs, Traffic Signals, and Lighted Arms. They're designed and constructed in the USA which means a lower carbon footprint with no overseas shipping involved. Also, our unique gearbox allows for full rotation and low wear, which translates to fewer repairs.

Protect vehicles from damage with the Signaling Aluminum Arm which is lit with red LEDs to send a clear signal for drivers to stop. When the Arm is raised the LEDs transition to green – clearly alerting drivers when to pull forward. The arm includes a built-in edge sensor to help prevent damage.

The Pedestrian Protection System helps keep walkers from harm, it will raise the Arm if a person is detected in the path of the barrier.

**DKS**  
DOOR KING®

**MADE IN USA**

SEE IT IN ACTION AT:

[doorking.com/trafficcontrol](http://doorking.com/trafficcontrol)

800-673-3299 • [info@doorking.com](mailto:info@doorking.com)

*\*Optional add-on feature.*



# The Growing Mobile Revolution in Access Control

Mobile credentials are slowly but surely becoming the next technology disrupter in access control

by Jeff Bransfield

In an increasingly technology-dependent society, individuals are looking to leverage their smartphones as much as possible, and mobile credentials can be helpful for both operational and security purposes. Mobile credentials can offer numerous advantages over traditional keys, cards or badges, and can often serve as a more secure and convenient alternative.

With COVID-19 still generating uncertainty in businesses reopening, and employees returning to the office, mobile credentials are a touchless, cost-effective, and convenient option for organizations looking to streamline their security while saving costs on hardware. However, it's important to note that COVID-19 is not the only reason so many eyes are fixated on this emerging trend in access control.

More people are using their smartphones now more than ever to open doors. And 2022 is likely to be a significant year for mobile credentials, whose market size and deployment are expected to reach entirely new heights. According to Gartner, Inc., by 2022, 70% of organizations adopting biometric authentication for access in the workforce will execute it via smartphone apps, regardless of the endpoint device

being utilized. Considering this figure was fewer than 5% in 2018, you can see how drastically things are changing.

In access control and identity management, individuals receive authentication from three varied factors, what they carry with them (keys, cards, and badges), their knowledge (pins or passwords), and what makes you, you (biometrics). In terms of the "what you carry with you" factor, smart readers, keys, and badges have been in use for a lengthy amount of time, whereby the user either taps their key, card, or badge on the reader or brings the card close to it.

However, mobile credentials, or the user's credentials stored in the user's smartphone, which can interact with the smart reader, have become a prevalent concept and are increasingly being deployed in numerous end-user organizations such as businesses, college campuses, hotels, and healthcare facilities.

What are some of the driving forces behind the adoption of mobile credentials?

## Convenience

Can you remember the last time you left for work without your cell phone? With how dependent everyone is on their



devices, there's a pretty slim chance it will be forgotten at home. Unlike an additional key card or badge, utilizing mobile credentials means one less item that a student, staff, or employee needs to bring with them each day. Smartphones also allow for a much simpler process in assigning credentials. Typically, when generating credentials in an organizational setting, whether, through keys, badges, or cards, each option requires workers or students to be physically present in an office to receive their credentials. This is not the case; users don't need to be physically



Courtesy of Getty Images -- Credit: Andrey Popov

*More people are using their smartphones now more than ever to open doors.*

present or even in the same building to have credentials assigned.

Additionally, as mobile devices have multi-factor authentication, like fingerprints, passwords, and facial recognition built-in, there is an added layer of security without the need for new hardware. Smartphones also incorporate location services, alleviating the need to scan a physical badge and allowing proximity servers to identify when an individual is near the door they have access to.

### **Security and Identity Protection**

Because smartphones have become so intertwined with daily life, most individuals tend to notice if their phone is no longer within reach within just a few minutes. This fact is ideal for maintaining secure premises. Physical badges, keys, or ID cards that sit in a purse or pocket all day without a second thought could take hours or even days for that individual to realize it's lost.

This gap in time creates an opportunity for someone to enter a building improperly, and when accessed, the system wouldn't recognize that the individual is not who they say they are. However, mobile access control creates a different timeline of events. When individuals notice their phone is missing, they can report it, and the credential can immediately be revoked to prevent a security event. It's also important to note that the mobile credential is not accessible until the access control app is launched,



meaning the digital badge will not be on display for the imposter to use.

In addition to quick response times and the remote revoking of credentials, smartphones typically store identifying information behind password-protected screens. For example, if an individual's ID badge, card, or the key gets lost, anyone who picks it up will know what that individual looks like, where they are located, and where they work or attend school. Suppose password protection is vital to your organization's needs; in addition to the first layer of password protection, you can require an additional password to access the credentials app on the smartphone as a preventative security measure.

### Cost

Mobile credentials can significantly reduce the expenses associated with physical badges, keys, or cards by eliminating the process of rekeying or key duplication. Not only can this be a sizable saving for larger organizations like hotels or college campuses that must replace keys regularly, but it serves as a flexible, sustainable, and scalable solution for many institutions. A mobile credential also won't end up in a landfill at the end of its life, meaning it's a greener option as well.

In addition to being more convenient and cost-effective to the organization, mobile credentials are a genuinely suitable option for end-users. Much like cards, keys, or other physical access control forms can be tied into any closed-loop payment system (commonly found at healthcare, hotels, and campus environments), mobile credentials can be as well. This feature serves as a convenient solution for users who want to combine their access control with multiple functions such as dining payments, library privileges, or room charges.

### Sustained or Temporary Access

Mobile credentials can serve as a long-term solution for an individual or as a quick and convenient option for contractors, visitors, guests, and anyone who would need temporary access inside an organization. As long as the visitors have the app-enabled on their smartphone, the proper administrators can digitally issue keys before their arrival and revoke them just as quickly.

### Potential Mobile Credential Barriers

Similar to contactless payment via debit cards and phones, mobile credentials are still an emerging technology that is continuing to be evaluated by early adopters. While it can serve as an incredibly convenient and scalable solution for an organization, it's important to consider the percentage of the organization's population that uses smartphones and ensure that they are Near Field Communication (NFC) enabled. As a side note, if this is a concern, there are the options of refitting older models with a special NFC phone case to bring them up to standards.

Mobile credentials  
can offer numerous  
advantages over  
traditional keys, cards  
or badges...

Mobile credentials  
can significantly  
reduce the expenses  
associated with physical  
badges, keys, or cards  
by eliminating the  
process of rekeying  
or key duplication.

Before completely adopting mobile credentials as the new form of access control, it might be beneficial to test the solutions with a target group to study the results first. However, if most of the population already uses smartphones, adopting mobile credentials would be ideal for pooling all-access credentials into one simple application.

### Access Control of the Future

"Mobile credentials are slowly but surely becoming the next revolution in access

control. Whether your organization is looking to switch immediately or in the near future, it's vital to keep a watchful eye on your security infrastructure now.

If your organization is currently overhauling its access control system, and even if mobile access isn't entirely on your radar at the moment, select options that will allow you to migrate to mobile and NFC-enabled devices in the future. Selecting an open and flexible system will ensure smooth adaptation for smart devices for future use.

Also, it's essential to search for smart readers that can identify several types of credentials. Using an open-architecture solution that verifies multiple sources of contactless credentials and encryption is vital if biometrics are necessary to your organization. With all of this being said, the question that begs to ask is whether or not mobile credentials will replace all physical keys and cards?

The answer depends on the specific organization's budget, comfort level, and population of employees, staff, or students that carry smartphones. In conclusion, if your organization is searching for a new access control solution or is on the fence about mobile credentials, make sure to search for manufacturers who offer scalable, flexible, and open-architecture solutions that can support mobile credentials. This proactive step will create a future-proof security solution that will serve your organization for many years to come. **AC**

### About the author:

Jeff Bransfield has been with RS2 Technologies, an ACRE brand, for more than eight years, currently serving as Vice President of Business Development. Jeff has been instrumental in elevating the RS2 brand to a leader in providing smart access control solutions, with double-digit sale percentage increases every year since 2009. After his first experience with the security industry working with DH Pace Systems Integration, he spent a year doing outside sales with Anixter, which helped him close the loop on the networking aspect of the industry.



# THE SMALLEST ELECTRIC STRIKE IN THE WORLD

# 323478LC

## THE COMPLETE CYLINDRICAL SOLUTION



**3 Faceplates 1 box solution**  
**Grade 1 construction**  
**1 inch total backset**



The strike kit that  
fits where other's can not,  
performs like other's will not.

**TRINE**  
ACCESS TECHNOLOGY.

Request information: [www.SecurityInfoWatch.com/10215438](http://www.SecurityInfoWatch.com/10215438)



[TRINEONLINE.COM](http://TRINEONLINE.COM)

**BUILT IN AMERICA, BASED IN AMERICA, BUY AMERICA!**



# New Standards Help Deliver a **Mobile Future for Access Control**

by Vincent Dupart



**A** successful access control project requires a collaborative effort among end users, and experts and employing industry standards

The demand for contactless access control solutions is increasing. The challenge is to offer a seamless user experience without affecting the corporate security level. The ubiquitous smartphone brings immense potential for new access control uses and better integration in our daily lives. Always available virtual badges are easier to use, reduce loss and theft and speed up access processes. And worldwide standards are helping to make scalable mobile solutions a reality today.

### Cyber and Physical Threats

The mobile workforce is here to stay.

This year, Strategy Analytics predicts the global workforce will have 1.87 billion mobile employees, 42.5% of the total workforce. More mobility brings an increase in threats with the IT infrastructure of both large and small organizations often subject to attacks in both the physical and digital world. A nefarious person with physical access to the corporate server room or a workstation connected to the network may access critical IT systems with disastrous consequences. The complete infrastructure may be taken hostage or made inaccessible, which will impact all business processes and endanger the continuity of the organization. Ninety percent of companies believe their data is at risk.

The loss or theft of sensitive and confidential data may also have serious financial implications or result in damage to the company's reputation.

Securing the corporate IT infrastructure and systems should not only be about information security. The physical security of IT facilities and any physical access points to the network should be an integral part of security planning and policies.

Today, more than ever, security and access control systems need to be flawless and standardized.

Numerous organizations are still using outdated technology (125 kHz, MIFARE Classic, HID iCLASS). Yesterday's access control solutions lead to higher maintenance costs and difficulties finding replacements as standards are adopted. A bigger concern is the physical badges can be easily copied using equipment readily available online. These security flaws impact the integrity and security of data. Again, flawless security is critical to a healthy enterprise.



*The ubiquitous smartphone brings immense potential for new access control uses and better integration in our daily lives.*

Courtesy of Getty Images -- Credit: Zephyr18



## Access Control Management Instantly Simplified

The management of physical access cards can be a daily headache. Hand delivering access badges to users, the hassle and security risk of lost badges, and the timely revocation of access rights are just a few of the activities taking up a manager's time.

Instead of presenting a physical badge to the access control system, users can now present their mobile credentials to the reader. Just bring your phone and you will get access to buildings, rooms, sites, and other secured zones that you have been authorized to access. The reality is that 98% of employees consider access control to be obstructive at times. Considering that we pass through an average of 11 accesses per day, there are many opportunities to reduce friction between access control and employees.

Virtual badges greatly reduce the time required for access management and offer so many additional benefits. By transferring the access badge to a smartphone for visitors, subcontractors and employees, your organization will instantly simplify card management! The creation, distribution and revocation of virtual access badges can be executed immediately, at any time, at any location in the world. People can start using their badges right away. And when their access rights are no longer valid, revoking the badge is a piece of cake. Digital access cards are much more effective and flexible for both users and managers. New apps allow users to store multiple digital ID cards so they're always accessible.

An important point to keep in mind: the cost of a virtual badge is two to five times less than that of a physical badge. A recent study demonstrates that over 50% of the operational costs of physical card management are related to printing, customization and distribution of the cards. With virtual badges, no more consumables, no more printing and personalization costs, no more recycling costs, and no more expenses related to loss or damage. Instead, your company will benefit from economies of scale and greater operational efficiency, in an "eco-friendly" fashion. The benefits of mobile are abundant and apparent to many. In fact, industry leaders estimate that 75% of business is already migrating to virtual credentials.

## With Secure Mobile Solutions, Possibilities are Endless

Understandably, new technology adoption can bring fear of complicated organizational operations and more work for an already

burdened IT department. While the need for a high-security system is obvious, the implementation may be overwhelming. The modularity of an access control system helps break down the barriers.

## Virtual badges greatly reduce the time required for access management and offer so many additional benefits.

Why? A modular reader can be adapted to meet future needs: the system can evolve toward the use of QR-codes to facilitate visitor access, use of a smartphone as an access key, or add an additional layer of security by integrating smartphone biometrics. And with mobile comes many possibilities for value-add solutions like combining identity management and access to printing solutions, leisure and event subscription solutions, etc. The smartphone can bring new possibilities for mobility.

Vehicle identification is another perfect example of a seamless process that expedites security and operations. A smartphone can automatically identify the vehicle and/or its driver, allowing vehicle access control to be as seamless and instinctive as the high-security identification of individuals. With the smartphone, access can be controlled in real time, ensuring that the vehicle can enter the parking lot and that the driver is fully authorized to do so.

But this need for intuitiveness must not be at the expense of security. It is crucial to guarantee the protection and confidentiality of data.

## Standards Help Mobile Access Control

With mobile devices – both iOS and Android – being used in high-security buildings, car parks and more, technology standards are crucial to ensure that security is never compromised.

Standards allow interoperability and they support the fight against "technological obscurantism". Industry standards are absolute necessities today to help clients compose their best-of-breed security solutions. Security departments are becoming aware

of the importance of choosing trusted technologies that guarantee certified and interoperable security. System integrators and solutions providers encourage their user partners to select the access control, security management solution or any other security-related system that best matches their requirements. Faced with the growing threats of physical and cyber-attacks, it's important to provide flawless security, based on OSDP and SSCP protocols.

Indeed, the Security Industry Association (SIA) Open Supervised Device Protocol (OSDP™) standard for access control security has been key to providing a first level of uniform security worldwide. Industry leaders have worked with the International Electrotechnical Commission (IEC) to create these stringent global standards.

Definitely secured by design, the communication protocol SSCP guarantees the protection and confidentiality of data and that customers are in full control of their application and their security keys.

## Teamwork Needed for Successful Mobile Access Control

A successful access control project is based on real collaboration between end users, and experts and the employment of industry standards. It must match your company's needs and requirements from development to implementation.

How can this be achieved? It starts with a complete and thorough analysis of the access points, the technologies in use, the required security levels and the practical use cases. Only after the needs are clearly defined and a roadmap is created should the project begin. Then your organization can move toward a high-security access control system that will successfully mitigate security risks while improving adoption, ease of use and overall operational efficiency. **AC**

## About the author:

Vincent Dupart is the CEO of STiD, a solutions provider that designs readers and credentials that offer all the tools that Chief Security Officers (CSOs) need to work independently in managing their security.

The company's mission is to promote trust and ease of use in the digital world.





DISCOVER  
HOW ACCESS  
DIFFERS



THOUSANDS OF PRODUCTS

DECADES OF EXPERTISE

UNBEATABLE SERVICE

For over 25 years, Access Hardware Supply has served as your partner in electronic and mechanical door hardware. From mechanical solutions that stand the test of time, to electronic ones that report every bit of information you need to keep your team safe, Access Hardware Supply has you covered.

Request information: [www.SecurityInfoWatch.com/10722906](http://www.SecurityInfoWatch.com/10722906)



**WHERE SERVICE MEETS EXPERTISE**  
IN MECHANICAL AND ELECTRONIC DOOR HARDWARE

**VON DUPRIN**

[accesshardware.com](http://accesshardware.com) | (800) 348 - 2263



# Even Small Access Control Jobs Translate Into **BIG BUSINESS**

Most access control systems cover fewer than eight doors

by David Ito



*Many opportunities  
abound in small  
access control  
applications.*

*Courtesy of BigStock.com --  
Copyright: AndreyPopov*



# Access the Exceptional.

For over 65 years, customers have trusted Alvarado and our U.S.-manufactured products to protect their assets and control the seamless flow of people. Now, with the added resources and support of dormakaba, we are a turnkey partner with the power to make your next project exceptional.

Contact us today and let our solutions experts bring your vision to life.

[ALVARADOMFG.COM](http://ALVARADOMFG.COM)

 **ALVARADO**  
dormakaba Group

Request information: [www.SecurityInfoWatch.com/12304402](http://www.SecurityInfoWatch.com/12304402)



**M**any security professionals who focus primarily on small one- or two-door access control jobs have come to realize that less can, in fact, be more. Although elaborate access control projects can be more lucrative, they require a larger investment in time for setup and training. Consequently, savvy security pros who take on the smaller jobs can remain as profitable and competitive as larger integration companies by focusing on this one- and two-door market niche.

It's a known fact that of the 80-20 rule, 80% of access control systems cover fewer than eight doors. And now with the availability of door controllers that use apps, there's no need for extra computer hardware or subscription-based software to maintain simple access control applications.

Enterprise-level access control systems simply can't get down to a price level of controllers that use smartphone apps. In reality, most end users just don't have to have nearly 90% of the capabilities of an enterprise system, which makes a simple app-based door controller a much better fit for their requirements and their budget.

Certain end users typically require single- or two-door installations – those who have to share a restricted space and who want access control features that aren't provided by simple key locks. One-door access systems often are implemented for single-room or single-unit environments in shops, condos, apartments, garages, or warehouses. Electronic access control can add and delete user access to a building or yard while providing defined schedules and a historical audit trail for reporting.

A one-door access control system can be used either as a stand-alone system or as one that's integrated with a larger access control system through different communication interfaces, such as TCP/IP, RS232 or other wireless technologies. Demand for stand-alone or integrated systems really depends on the marketplace and application, but networked systems require a substantial investment, whereas a stand-alone system can be implemented within hours. Integrated networks deliver a higher level of security where intrusion, elevator control, audio communication and visual surveillance systems are necessary. The majority of small systems don't require those extra layers of security.

## Single-Door Components

Ideally, a single door access control system should include an electric door lock,

a controller, an entry reader and an exit reader, a door-position switch and a robust battery-backup power supply. As referenced above, communication ports should include RS232, RS485, USB, TCP/IP or other wireless protocol interfaces to facilitate integration with a networked access control system as necessary and to allow for potential expansion. In addition, a single-door access system should include alarm annunciation via audio speakers or alarms or strobes and be easy to install and to operate.

Essentially, all the features of a single-door system are the same as those of a two-door system, but with the added capability of creating a mantrap or interlock system where one door must be closed before the other door can be opened.

And, given the increased demand for Bluetooth readers and mobile credentials, one- and two-door access systems today should be able to support various reader types, particularly mobile smartphones that use BLE or Wi-Fi, in addition to biometric, proximity and keypad credentials.

Manufacturers over recent years increasingly have rolled out various business models for Bluetooth readers. Some require a yearly subscription or charge per credential to the user, and others are available at no charge to the end user. Unfortunately, the acceptance and adoption of Bluetooth readers have been colored by conflicting information that's been somewhat confusing to installers and end users as to the real cost and benefit of implementing the technology.

However, given all the technological advances packed into a modern smartphone, smartphone readers likely will become the norm fairly soon. Bluetooth is only one of many wireless protocols being developed for smartphones. Multilevel authentication — using a combination of something the authorized user has, knows and is as credentials — also is built into the system by using a high-end smartphone because smartphones can open through the use of facial recognition or a fingerprint along with a PIN before an app can be used.

Furthermore, the prevalence of smartphone apps has enabled the industry to leverage the processing power of smartphones to provide encrypted authentication to a reader that's wired to an access point. The same technologies used for tracking smart tags for Apple or Samsung phones are being developed for access control applications. Through the use of apps, it now

is possible to harness the capabilities of a computer, so single- or double-door controllers no longer require a dedicated computer and all its accompanying hardware and software — and personnel to manage it — to configure the controller.

## Secure Your Success

Security technicians and locksmiths who serve the single- and double-door market should know the unique advantages of access control capabilities versus a key lock to comfortably and confidently demonstrate the benefits to their customers. Having simple low-voltage wiring skills and awareness of the types of power that can be used will prove beneficial to the security pro.

To increase sales, they should convey to their prospects that there are new, innovative and low-cost means of providing simple access control without the necessity to learn complex software on a computer. Apps are designed to be intuitive, which allows authorized personnel to use their own smartphone to configure the controller, add or delete users, set schedules and even enable their users, such as tenants or employees, to use their smartphone as an access credential.

Choosing a strong access control technology manufacturer also is critically important. The products they offer should meet all federal regulatory requirements, including FCC and UL for power supply. All of their resource material should be free and also meet all federal regulatory guidelines. A true and trusted access control vendor partner should deliver superior technical support, product delivery and a top-notch warranty.

Many opportunities abound in small access control applications. Indeed, they can translate into big business and prove that less absolutely can be more. **AC**

## About the author:

David Ito is a product manager for Camden Door Controls and has more than 25 years of product development experience in security and access control, fire detection and nurse call systems. Ito has worked for many multinational manufacturing firms throughout his career in a product development and marketing capacity and is a certified pragmatic marketer.



WE ARE THE INDUSTRY SOURCE  
FOR ACCESS CONTROL PRODUCTS,  
AT THE ABSOLUTE LOWEST PRICES.



Request information: [www.SecurityInfoWatch.com/21143796](http://www.SecurityInfoWatch.com/21143796)

OVER 200 BRANDS IN STOCK, OVER 30,000 DIFFERENT ITEMS TO CHOOSE FROM!

ALARM LOCK    TRINE ACCESS TECHNOLOGY    The Guard    LOCKLY    SDC    CAMDEN DOOR CONTROLS    ZKTeco    pdk    ROSSLARE    SECO-LARM    Adams Rite    BALDWIN



3301 N 29th Ave, Hollywood, FL 33020  
sales@uhs-hardware.com  
UHSHardware    UHSHardware    UHSHardware

Got Questions? Call Us  
**1-800-878-6604**





*PACS deployed across large-scale corporate campuses generate thousands of alerts a day, with more than 90% reporting as false alerts.*

*Courtesy of Getty Images*

# AI in Security:

## The New Era of Access Control

Innovations in computer vision and AI can be augmented to create an efficient and actionable approach to perimeter security

by **Shikhar Shrestha**

**A**l is improving industries virtually across the board — from helping to better detect lung and breast cancer to extend the life of machines through predictive maintenance. By pattern matching at scale and automating mundane tasks, AI is enabling experts to focus on what they do best.

AI has already been cemented into most companies' cybersecurity posture. Cybersecurity professionals are using AI to detect and easily solve malicious network behaviors quickly, with 83% of organizations stating that they wouldn't be able to deal with cyberattacks without AI.

### **What About AI for Physical Security?**

This begs the question: why is physical security lagging so far behind cybersecurity in the adoption of AI? For physical security professionals, AI has the ability to transform how they respond to threats, moving from a largely reactive posture, in which teams

# Introducing XS4 Original+

The XS4 Original+ is the next generation of SALTO's most trusted and widely used electronic locks—now including Hardware Secure Element (HSE) technology.

Get the latest security features and advanced capabilities with shorter product delivery lead times.

Learn more at [salto.us](https://salto.us) or call (866) GO SALTO

**SALTO**  
inspired access

Request information: [www.SecurityInfoWatch.com/10225529](https://www.SecurityInfoWatch.com/10225529)





respond to threats after they happen, to a proactive posture, in which risks are automatically detected. This enables security professionals to intervene before an incident escalates or even occurs. For the business, proactive physical security can reduce operation costs, improve employee retention and, most importantly, result in better protection of people and assets.

There are certain physical behaviors that indicate a perimeter security threat, like someone jumping a fence, spoofing a badge at a secure entrance, forcing a door open or tailgating. Each action indicates a pre-incident security threat that could negatively impact people or assets if left unchecked. Leveraging AI, we have an opportunity to identify these threats early, rather than waiting for the security incident to happen.

Incidents tend to follow predictable patterns of smaller instances of threats, which have signatures of physical human movement. Until quite recently, human effort was required to pattern match these behaviors. Someone would need to see the threat behavior happen, either in-person or via surveillance feed. Or an alert might be raised by a physical access control system (PACS), which then requires a human to verify the legitimacy of the alert. AI can solve this very time-consuming task, enabling security teams to focus on responding to threats before they escalate.

As an example, let's look at a relatively large corporate campus with 300 security cameras and 500 doors connected to PACS. Because PACS are relatively simple and constrained to tracking hardware events such as badge reads, they are unable to provide the context security teams need to accurately detect threat signatures. A PACS alert indicating a door being forced open by an intruder looks the same as a strong gust of wind or a faulty maglock.

## Let AI Do the Work

PACS deployed across large-scale corporate campuses generate thousands of alerts a day, with more than 90% reporting as false alerts. These false alarms could be triggered by a door held open for just a moment longer than expected or by an invalid badge alert caused by a faulty read. As a result, a human must visually confirm each alert – resulting in a huge manual lift.

Many companies have policies that require security teams to verify the validity of each alarm. According to customer interviews,

dispositioning false alerts for a relatively large corporate campus equates to 8,000+ hours each year. That is the equivalent of four full-time employees. At these volumes, security teams often succumb to “alert fatigue,” which leads to a slower response to alerts or alerts being missed altogether. This increases the likelihood that a legitimate security threat goes undetected.

The simplicity of false alarm patterns makes PACS a prime candidate for AI-powered automation. Using AI to tap into existing PACS and camera surveillance systems enables these types of events to be automatically dispositioned. The combination of connectivity to pre-existing hardware systems, AI and computer vision is a solution recently introduced to the market called computer vision intelligence.

---

“Incidents tend to follow predictable patterns of smaller instances of threats, which have signatures of physical human movement.”

---

It combines the visual verification of computer vision with the pattern matching capabilities of AI to monitor existing surveillance video feeds instantly and accurately detect threat behaviors at any scale of campus. Computer vision intelligence triages incoming alerts on behalf of security teams, significantly reducing the volume of alerts and providing more time for security personnel to act.

Computer vision intelligence effectively becomes the software brain for the signals that hardware-centric security tools create. If cameras are the eyes and PACS are the ears, computer vision intelligence is the brain that turns those signals into actionable information.

Early adopters of computer vision intelligence, such as VMWare, have been able to reduce alarm volumes by 93% and reduce hard-to-detect threat behaviors like tailgating by more than 99%. Similarly, NorCal Cannabis is able to prioritize alerts based on the requirements of a wide variety of locations — from growing facilities to retail stores — by leveraging this technology. For example,

a door propped open at a warehouse during the day is much less concerning than if a door is propped open in the middle of the night. Computer vision intelligence is able to understand the context and treat each of those situations differently. When connected to a triage system, it can also initiate the proper escalation path, ensuring fast and effective response and dispatching.

## AI Drives Innovation

The industry is just now catching on to the value of integrating security systems with layers of intelligence, creating a whole new market of startups. In fact, Grandview Research predicts US Enterprises will spend \$171 billion per year by 2027 to secure people, places and physical assets. The industry growth not only reflects an increasing demand for innovation in physical security but also shows broader promise that with additional resources this technology will be able to deliver significant advancements in the coming years.

PACS and security cameras create a foundation for enterprise access control. Now, with innovations in computer vision and AI those tools can be augmented to create an efficient and actionable approach to perimeter security. Security teams can focus on responding to and preventing security incidents rather than monitoring surveillance feeds and dispositioning false alerts. The existing investments companies have made into cameras and PACS become even more effective as physical security enters a new era of AI. In tandem, security professionals are empowered to better protect people and assets. **AC**

## About the author:

Shikhar Shrestha is the CEO and Co-Founder of Ambient.ai where he leads the company in scaling its technology with the mission to prevent security incidents before they happen.



Shrestha holds a Master of Science in both electrical and mechanical engineering from Stanford University and prior to co-founding Ambient.ai, held engineering positions at both Apple and Google. Since co-founding Ambient.ai, Shrestha has led the company through the Y Combinator Winter 2017 cohort, raised \$52.2 million in venture capital funding from a16z, secured enterprise customers across industries, and launched the company in January 2022.



*If your* **ACCESS CONTROL**  
**PROJECT**  
**HINGES** *on*  
**SPEED**  
*we'll*  
**HANDLE** *it.*



**No Matter what your project hinges on, we can handle it**

From complex projects to repeat orders, we'll deliver the right ASSA ABLOY solution for you so you can focus on what's truly important: driving your business forward.

**banner**   
SOLUTIONS™  
**ASSA ABLOY**

[bannersolutions.com](http://bannersolutions.com)

888.362.0750

Request information: [www.SecurityInfoWatch.com/12071932](http://www.SecurityInfoWatch.com/12071932)



# 5 reasons why faces are superior access control credentials

Improved accuracy and benefits provided by today's facial recognition tech make it an ideal primary user authentication tool

by Aluisio Figueiredo



(Image courtesy World Image/bigstockphoto.com)

Professional security practitioners know that the best approach for the highest level of identity confirmation is to use multi-factor authentication made up of something someone has – such as an access card, something someone knows – such as a PIN code, and something someone is – such as a fingerprint. Combining these methods delivers a level of assurance that is entirely suitable for situations that involve national security, nuclear weapons, and other important matters.

But this approach is overkill for most access control systems. The vast majority of access control systems are used for everyday purposes at business offices, factories, campuses and housing facilities, and similar venues. These facilities all require dependable, high-accuracy identity

*Facial recognition as a credential is the ideal solution for organizations looking to deploy the most current, accurate, and rapid technology while simultaneously enhancing the user experience in most access control applications.*

# Every Access Control Solution

# One Brand



Mobile



Cellular



Cloud



Wireless Locks



Embedded



Enterprise

## Wireless Online Locking



## Embedded, All-in-One Controllers



## Integrated Enterprise Platform



- ▶ Free & Easy Mobile Credentials
- ▶ Global Lockdown
- ▶ Cell-Networking, WiFi or POE
- ▶ Hosting/Monitoring Option
- ▶ App & Realtime SMS Alerts

- ▶ Web Browser-Based. No Software
- ▶ 1- to 4-Door Modular Controllers
- ▶ NFC, Prox, BLE, HF/Mifare Readers
- ▶ Systems from 1-128 Doors, up to 64 Panels
- ▶ Over 500 Doors with 2nd Server

- ▶ Access Control, Security Locking & Video Management from Anywhere
- ▶ Infinitely Scalable, Lowest Total Cost of Ownership
- ▶ Dynamic Map Control
- ▶ Local & Remote Monitoring
- ▶ Threat Level Management
- ▶ Active Shooter Detection

# Continental Access

**Get Started** Join the Napco Pro Certified Dealer Program



call 1.800.645.9445 or email [CIMktg@ciaccess.com](mailto:CIMktg@ciaccess.com)  
[www.ciaccess.com](http://www.ciaccess.com)

Request Information: [www.SecurityInfoWatch.com/10213301](http://www.SecurityInfoWatch.com/10213301)



confirmation while also controlling cost and processing users quickly and efficiently.

So, the question is: what is the best credential to use for fast, accurate access control identity authentication? The answer – facial recognition.

Facial recognition as a credential is the ideal solution for organizations looking to deploy the most current, accurate, and rapid technology while simultaneously enhancing the user experience in most access control applications.

From unlocking mobile phones to identifying criminals on the run, facial recognition technology continues to be the technology of choice in a variety of use cases that require the utmost level of personal identification and authentication. It is therefore no surprise that facial recognition is being widely adopted as the superior form of access control credential. Faces as access control credentials offer many benefits that ID badges, passwords, proximity cards, mobile devices, and other biometrics simply cannot.

Here are 5 reasons why facial recognition is the right choice for access control identity verification:

## 1. Facial Recognition can Integrate with Every Access Control System

Every access control system (ACS) requires some mechanism to evaluate access requests and determine whether the applicant has permission to access the controlled resource. In the past, keypads and access card readers were the most common way for a user to request access. Because facial recognition systems can provide the same kind of authorization signals to an access control system as these older methods, they can integrate with every ACS.

Facial recognition systems turn any person's face into their credential. Faces can be used as either a standalone solution for access, or they can be combined with other credentials for added security as a source for multifactor authentication.

## 2. Faces are Frictionless and Touch-Free

When a person's face is their credential, there is no need to touch anything to receive access. No keypads to enter PIN codes on, no fingerprint readers to touch, and no phones or handheld credentials to scan. Users only need to glance at a reader, and, with the proper permissions, the door is unlocked. This reduction in touch surfaces reduces the potential spread

of germs and harmful bacteria, therefore promoting a safe and healthful workplace.

As mentioned above, facial recognition seamlessly integrates with existing access control systems, so organizations can replace their access control touch points without having to rip-and-replace an entire system. Implementing a touchless access process also keeps a facility's employees and visitors moving, since people are no longer stopping to find their physical credentials or enter their PIN codes. In this way, facial recognition provides a frictionless access experience that limits close contact and promotes social distancing, while improving operational efficiencies by reducing wait times at entry points.

## 3. Facial Recognition is Accurate and Fast

The most advanced current facial recognition technologies make use of powerful computing technologies to deliver precise recognition accuracy faster than ever before. Maintaining a high percentage of correct recognitions in a range of viewing conditions is essential for access control applications, so only facial recognition systems that make use of the latest AI and processing technologies provide the most reliable and accurate solutions.

Fast processing also supports a fast enrollment process, whether when enrolling new users or leveraging an existing database, and provides a better user experience.

For example, Intel's ANN algorithms, which are being leveraged by some facial recognition platforms today, also allow for extremely fast processing.

## 4. Faces Can't Be Lost, Forgotten, or Stolen

Unlike physical access control credentials, a user can't forget their face at home, drop their face in the parking lot, or loan their face to someone else. A user's face is always with them and with nothing to carry, there is nothing to lose, forget, or steal. Replacing lost or stolen credentials such as badges or key fobs is costly, not to mention an administrative hassle. Organizations that solely rely on facial recognition as an access control credential eliminate the manual tasks associated with printing, issuing, and re-issuing physical credentials.

Lost or stolen credentials also pose a significant security risk. Organizations looking to enforce a zero-trust environment may have a hard time doing so when physical access

credentials are easily lost, stolen, and shared, often without the owner even knowing.

The loss of physical credentials due to theft or carelessness places an undue burden on security administrators who must stop their workday to restrict the lost credential's access, then issue a new credential. Such problems are eliminated entirely when facial recognition is the single source of truth for an access control system.

## 5. Facial Recognition is Highly Secure

Some low-quality facial recognition systems, and those using outdated technology, can be fooled by hackers or bad actors who hold an image or video of an authorized user up to the camera in an attempt at gaining access. However, most facial recognition providers today incorporate anti-spoofing features designed to detect and thwart these attempts.

Furthermore, facial recognition as an access control credential only works if a user consents to being enrolled in the system – that is, if users "opt in" to the service, and are never used for general surveillance. Such consent should eliminate potential privacy concerns, but some companies take extra steps to assure personal privacy. The most advanced systems do not capture or store any actual images of an individual's face, further ensuring privacy. Some systems also use encryption as an additional security layer to protect against unauthorized access to the system and database. All users' personal data is further encrypted both while in transit and at rest.

When compared to other traditional credentials such as physical access cards, PIN codes, and mobile credentials, facial recognition is the clear standout when it comes to facilitating a zero-trust environment. Modern facial recognition systems provide highly accurate, secure, and frictionless face-as-a-credential capabilities to access control systems, both new and existing, while maintaining individual privacy. Organizations looking to deploy facial recognition as a credential can expect increased operational efficiencies, decreased administrative tasks, and a streamlined access process that will ensure security while improving the user experience. **AC**

### About the Author:

Aluisio Figueiredo is the CEO of Intelligent Security Systems.



Opening New Doors to Innovation, Quality and Support!

# A WHOLE NEW LEVEL OF USER CONVENIENCE!

Select the best access control credential for each system user

TWO BUTTON FOB



MPROX BLE



CARD OR TAG



SMARTPHONE



Built-in Bluetooth® interface and App supports Android™ and Apple iOS™ smartphone access credentials.

Camden's remarkable CV-603 BLE two door access control system now supports smartphone credentials, right out of the box! No additional reader/interface required and there are no subscription fees.

Designed to provide maximum flexibility in small door and gate applications, CV-603 BLE comes ready to support each system user with the card, security FOB, or smartphone credential they want.

## FEATURES

- Supports up to 2,000 users
- Bluetooth® managed system configuration App
- Built-in 433Mhz. RF receiver
- CV-603PS controller with 1.5 Amp power supply and metal cabinet



1.877.226.3369 / 905.366.3377

[www.camdencontrols.com](http://www.camdencontrols.com)

Request information: [www.SecurityInfoWatch.com/10213140](http://www.SecurityInfoWatch.com/10213140)



By Steve Lasky

# Advanced Analytics is The Cool Tool for Access Control

by Steve Lasky

**T**he paradigm shift in physical security from a reactionary and defensive proposition to a more proactive stance has characterized the migration of advanced analytics into almost every platform. Security end-user demanding systems that are faster and more intelligent, and at the same time cost-efficient and better suited for integrated solutions, are looking for more than technology that simply detects and deters.

This improvement in security operations at the enterprise level is also addressing the convergence of physical and cybersecurity threats while easing the migration into a more defined digital world. As stated in a recent Security Industry Association (SIA) report: "Security will move beyond video surveillance and access control with features such as autonomous reporting, monitoring and response. Autonomous security systems will communicate with each other and with people and will act on their own to collect more information and trigger complex safety protocols. Security technology will operate with predictive intelligence and will be deeply integrated with building systems..."

## AI Solutions are Not Just for Video Surveillance

For example, says Sam Joseph, co-founder and chief executive officer of Hakimo, whose company develops software for the physical security industry powered by artificial intelligence (AI), "suppose you work at Google, or any big enterprise and you have offices in San Francisco and in New York, and suppose you are in the San Francisco office, or somewhere on the west coast, logging into your email using single sign-on or any other standard techniques. If someone uses your badge or a cloned badge of yours in New York, these two pieces of information are stored in completely separate systems. No one will notice that

there is no system connecting the two, and a security breach as obvious as this goes completely undetected today."

Joseph, like many technologists who have made their way into the physical security industry because they see a sector that is moving forward despite itself, contends that physical security systems have lagged behind cybersecurity advancements for the previous two decades because many systems operators are overwhelmed with incoming data and constant alerts that distract more than inform and that is more than most humans can manage.

"This was a problem that cybersecurity faced in the 2000s. Fifteen, twenty years ago when cybersecurity systems started generating a lot of alerts, there was no way a human analyst or a human operator could monitor them all effectively," Joseph continues. "Physical security has reached that point only now. And one reason convergence is getting delayed is that cybersecurity is way ahead in terms of tools and techniques. Physical security is still lagging behind."

## Access Control Systems Expand Capabilities with AI

AI software applications like Joseph and his team develop, with their data analytics algorithms, can also analyze alarms across time and diagnose faulty hardware, such as door sensors and sensors. Pointing out anomalies in cardholder behavior is a crucial tool for access control accountability. The software can point out impossible travel (the same card being used at multiple locations within a short duration which is physically impossible), unusual time or location of usage.

Those strengths have been more than tested over the last 24 months with the lingering COVID crisis that has staggered office time for workers and challenged

employers to provide an extra measure when it comes to duty of care. The mindset of what an access control system is and what it should do has been turned on its head. For Joseph, the present environment has been a motivating element for a changing technology segment.

"COVID was a significant change for the physical security departments within enterprises because everyone started turning to physical security and asking, 'How many people are there in the building today? What's our occupancy right now?' That data was always there in your Lenel database or in your C-CURE systems, but nobody cared to leverage it. This crisis has shown, in some sense, the value that the data sitting in these systems have in general for security, health and safety. It also showed how difficult it is to do something extremely basic," Joseph says. "We literally have talked to customers who were running reports daily in Lenel, exporting into a spreadsheet, and then copy-pasting the data into a different spreadsheet and before finally building graphs on their own tools to show how building utilization is changing across time."

Joseph continues that it is all about the software now. And when he and his company talk about software, it is an AI-driven solution. "We put zero hardware in the field. We just take in the existing cameras, existing access control systems and use our algorithms."

**About the Author:** Steve Lasky is a 34-year veteran of the security industry and an award-winning journalist. He is the editorial director of the Endeavor Business Media Security Group, which includes magazines Security Technology Executive, Security Business and Locksmith Ledger International and top-rated webportal SecurityInfoWatch.com. Steve can be reached at [slasky@endeavorb2b.com](mailto:slasky@endeavorb2b.com). **AC**



RECONASENSE

# A BETTER WAY

Access Control with Intelligence

Take back command of your facility with **the industry's only risk-adaptive access control and security management platform** – ReconaSense.

Our user-friendly platform evaluates data from across your enterprise to provide security operations with **real-time threat intelligence, risk-based permissions** and a suite of security automation capabilities.

Learn how you can use ReconaSense to **make better decisions, faster** while improving life safety and creating transformative business outcomes – all through a single pane of glass.



APL #10131

Our platform is FICAM certified and designed to federal specifications exceeding Government regulations for:

- HSPD-12
- ICD705
- UL294
- FIPS 201
- UL1076
- FIPS 140-2



**RECONASENSE.COM**

+1.512.220.2010 | [insider@reconasense.com](mailto:insider@reconasense.com)



ReconaSense is an American company headquartered in Austin, Texas.

Request information: [www.SecurityInfoWatch.com/10215136](http://www.SecurityInfoWatch.com/10215136)





# Simply Powerful. Powerfully Simple.

Access control for your customers to better understand and manage their facilities.



One Platform to Manage



Business Insights from Data



Mobile Credentials and Capabilities