ACCESS CONTROL 2023
TRENDS & TECHNOLOGY

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

Does Interoperability Matter **When Integrating Access Control?**

The short answer is yes, but it is crucial to know why and where
P. S12

TECHNOLOGY TRENDS

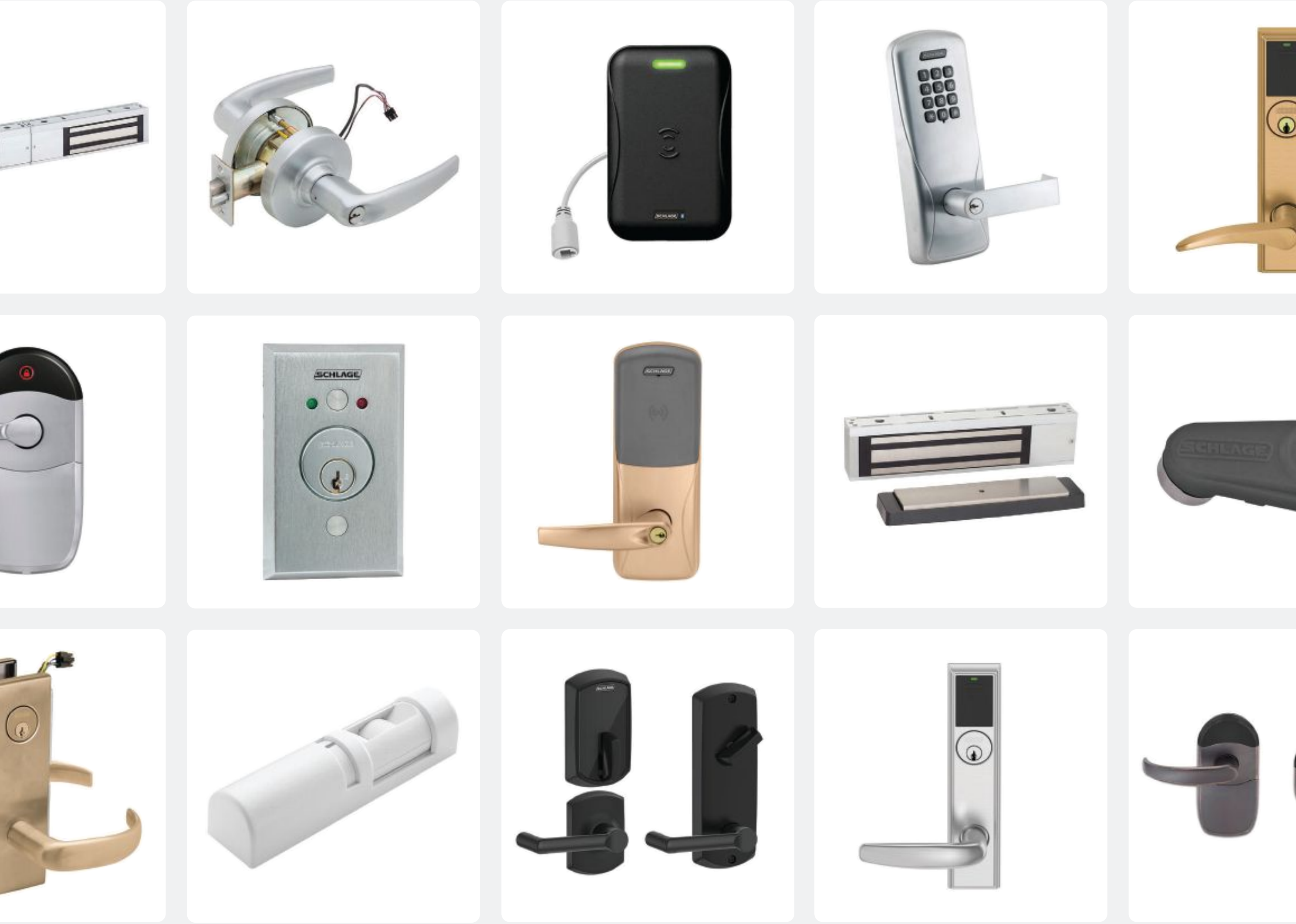
- How Cloud-Based Security Ignites Digital Transformation P. S16
- Multi-Factor Authentication is a Key for Secure Access Control P. S6
- How to Create a Seamless Video and Access Control System P. S22
- Keeping Access Control on Pace With Organizational Growth P. S26

www.LocksmithLedger.com | www.SecurityInfoWatch.com

July/August 2023

ENDEAVOR BUSINESS MEDIA

EVERYTHING SCHLAGE



SECLOCK.com **800.847.5625**

Request information: www.securityinfowatch.com/10215009

SECLOCK

SPEC ANY TECH.
CONFIGURE YOUR FIT.

INTEGRATED STROBES
REMOVABLE TOP PLATE FOR ADDITIONAL TECH
INTEGRATED CAMERAS
CUSTOMIZABLE COLORS AND DECALS
EMERGENCY
AXIS COMMUNICATIONS
PUSH FOR HELP
2N
USE ANY EMERGENCY CALL DEVICE
WALL STATIONS
PROGRAMMABLE LED LIGHTING
GROUND TOWERS

SAFE CITIES, SCHOOLS, AND PUBLIC SPACES

Pedestal PRO reinvented emergency call stations by bringing unlimited configurations with any tech you spec–networked audio and video, lighting, and branding of your choice.

Strong aluminum construction, but light weight for easy one-person installation. Ready in 15 days or less and shippable by UPS or FedEx.

GET YOUR FREE DEMO UNIT!

Free wall station demo for dealers. Contact us for details.

800.660.3072 | info@pedestalpro.com

PEDESTAL PRO®

TO LEARN MORE, SCAN QR CODE OR VISIT:
Pedestalpro.com/EmergencyCallStations
Request information: www.securityinfowatch.com/21130788

ACCESS CONTROL 2023
TRENDS & TECHNOLOGY

COVER STORY

ACCESS CONTROL

CRITICAL ISSUES

CODE COMPLIANCE

INDUSTRY INSIGHTS

DEPARTMENTS

ACCESS CONTROL 2023
TRENDS & TECHNOLOGY

PUBLISHED BY

ENDEAVOR BUSINESS MEDIA

30 Burton Hills Blvd, Ste 185
Nashville, TN 37215
800-547-7377
Access Control – Trends & Technology 2023 is a supplement to Locksmith Ledger, Security Business and Security Technology Executive magazines.

EDITORIAL

Editorial Director | Steve Lasky
Editor, *Locksmith Ledger* | Emily Pike
Editor, *Security Business* | Paul Rothman
Editor, *Security Technology Executive* | Steve Lasky
Editor, *SecurityInfoWatch.com* | John Dobberstein

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 | Erica Paquette
epaquette@endeavorb2b.com

ENDEAVOR BUSINESS MEDIA, LLC

CEO | Chris Ferrell
President | June Griffin
CFO | Mark Zadell
COO | Patrick Rains
CRO | Reggie Lawrence
Chief Digital Office | Jacquie Niemiec
Chief Administrative and Legal Officer | Tracy Kane
EVP/Group Publisher — Tech | Lester Craft

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

Endeavor Reprint Services
reprints@endeavorb2b.com

The Future is Now for Access Control

by Steve Lasky

The *Access Control Trends & Technology* supplement has been published by our security group for more than two decades now. And to say the industry's landscape has changed over the years would be an obvious understatement.

Back in 2008, our former SecurityInfoWatch.com editor Geoff Kohl, now the man admirably heading up the Security Industry Association's marketing staff, sounded the alert in a feature he wrote for our website about a hacker from the U.S. who reportedly breached the security on NXP Semiconductor's Mifare-classic proximity card chip. The smart card chips (which were Mifare Classic chips), were mainly used in facility door access control and inexpensive toll booth and transportation user applications.

This was a huge cause for concern among the access control community. It shook the confidence of physical access control card users because it was the first true hack of EAC card systems technology. My, how far we've come.

The spectrum of technology covered in the 2023 edition of this supplement runs the gamut from advanced technology residing in the cloud to cutting-edge applications of high-end biometrics and AI-powered solutions. Today, a hack signifies more than a college student being able to clone a prox card. The stakes are much higher with the proliferation of connected systems that are predominantly network-centric.

While our users, integrators and solutions providers still continue to reside in a mostly traditional world of access control technologies, the future is butting up against our lock and key analog history. We are destined to continue a rapid migration into a digitized environment where we are more reliant on artificial intelligence (AI) and data-driven analytics. Buckle up, the future is now. This edition examines how multi-factor authentication has become an integral part of many access control systems, and why organizations are seeing mass digital transformation as tech moves to the cloud. Integration is also a key factor for access control, especially when you consider your video surveillance needs. We invite you to read about it all. AC

Advertisers' Index

Advertiser Name	Page	WebSite URL
Access Hardware Supply	S33	www.securityinfowatch.com/10722906
Banner Solutions	S35	www.securityinfowatch.com/12071932
Camden Door Controls	S21	www.securityinfowatch.com/10213140
Continental Access – NAPCO	S40	www.securityinfowatch.com/10213301
DKS DoorKing Systems	S9	www.securityinfowatch.com/10213482
Dormakaba	S29	www.securityinfowatch.com/12304402
Farpointe Data Inc.	S31	www.securityinfowatch.com/10215927
NAPCO Security Technologies	S7, S15	www.securityinfowatch.com/10215125
Pedestal PRO	S3	www.securityinfowatch.com/21130788
SALTO Systems Inc	S37	www.securityinfowatch.com/10225529
Seclock	S2	www.securityinfowatch.com/10215009
STid	S1, S10-S11	www.securityinfowatch.com/12266353
Viking Electronics	S39	www.securityinfowatch.com/10556843

This directory is provided as a service. The Publisher assumes no liability for errors and/or omissions.

Multi-Factor Authentication is a Key for Secure Access Control

MFA significantly reduces the risk of unauthorized access and strengthens overall security posture

by Antoinette King, PSP, DPPS, SICC, CMMC-RP

With the rapid advancement of technology and the growing number of security threats, both physical and cyber, conventional methods of access control have become insufficient in ensuring the security of sensitive information and systems. Access control systems have traditionally relied on single-factor authentication, usually in the form of PIN codes, access control cards, or passwords. However, each of these credential mechanisms alone is susceptible to various types of attacks, such as brute force attacks, credential spoofing, and credential theft. Consequently, there is a pressing need for a more robust authentication mechanism that can withstand evolving security threats. To mitigate these risks, organizations and individuals are turning to multi-factor authentication (MFA) as a robust security measure. MFA combines multiple factors, such as passwords, biometrics, tokens, and smart cards, to provide an additional layer of security. While MFA is not a panacea for all security challenges, it is undeniably a powerful tool in the fight against unauthorized access. It is important to explore the effectiveness of MFA in securing access control, by discussing its benefits, limitations, and considerations.

PHOTO: 1370845936 | ARTEMISDIANA | GETTYIMAGES.COM

While multi-factor authentication is not a panacea for all security challenges, it undoubtedly provides a robust and effective approach to secure access control.

Multi-Factor Authentication (MFA) Explained

MFA is an authentication method that requires users to provide two or more independent factors to verify their identity. These factors typically fall into three categories: knowledge factors (something you know), possession factors (something you have), and inherence factors (something you are). Knowledge factors include something the user knows, such as a password or a personal identification number (PIN). Possession factors involve something the user possesses, like a physical token, a smart card, or a mobile device. Inherence factors refer to something inherent to the user, such as biometric data (fingerprint, facial recognition, etc.).

By combining multiple factors, MFA strengthens the authentication process and mitigates the risks associated with single-factor authentication. Even if an attacker manages to compromise one factor, they will still need to overcome the other factors to gain unauthorized access.

Save $100 with New Try-Me Offer

Tired of All the IT Delays On Access Control Jobs?

AirAccess®
by Napco

Get More Accounts Up & Online Faster & Earning RMR, with the Access System that Eliminates IT Headaches, *It's Cell-Based & Auto-Connects, Just Like Your Phone*

- Up to 2X the RMR on Small & Medium Businesses
- Easy Networking Powered by StarLink Cellular
- Flat $19.95 mo./System

FLAT RATE! $19.95 Monthly System Flat Rate Easy to Afford & Quote

Add More RMR-Accounts Faster

Central Station Monitoring Option-Doubles RMR*

Automatic Cellular Networking by StarLink

Cloud-Based Software & Easy 5-Step Wizard Configuration

Now Save $100 on Every AirAccess System Installation

App w/ Mobile Credentials: Use Wireless 1-Door Panels & Wiegand Readers

or Use Existing/New Trilogy Locks in Real-Time w/ Global Control & Lock-Down

or Wireless Designer, Customizable ARCHITECH models in choice of trims

NAPCO Access

Ask for AirAccess Starter Kit Today
Call 1.800.645.9445 *or* visit **www.AirAccess.com**

AirAccess, StarLink, Trilogy, Networx are trademarks of NAPCO Security Technologies. Monthly Flat System Base Rate of $19.95 in US Dollars; +$5.95 for CS alarm monitoring option.†

Request information: www.securityinfowatch.com/10215125

Benefits of Multi-Factor Authentication

MFA offers several advantages over traditional password-based authentication. It provides stronger authentication, and protection against password-based attacks, and offers scalability when implemented properly.

Stronger Authentication: MFA significantly enhances the security of access control systems by adding additional layers of verification. This reduces the likelihood of successful brute-force attacks, as the attacker would need to bypass multiple authentication factors. MFA provides a higher level of confidence in the user's identity, as it requires the possession of physical objects, knowledge of information, or the use of biometric data. This makes it harder for attackers to impersonate legitimate users. Finally, MFA can be easily implemented across various platforms and devices, offering flexibility and convenience to users.

Protection against Password-based Attacks: Considering that most applications require an email address as the user ID, and most email addresses are made publicly available on social media, websites, and business cards, attackers could potentially have 50% of the credentials to access those applications. Password-based attacks, such as brute-force and dictionary attacks, can be thwarted by implementing MFA. Even if a password is compromised, the additional factors required for authentication add an extra layer of protection.

Adaptability and Scalability: MFA can be implemented across various platforms, applications, and devices. It offers flexibility and scalability, with several different options for additional factors, making it suitable for organizations of all sizes and sectors.

Limitations and Challenges

MFA is not without its limitations. Challenges include increased complexity and potential inconvenience for users, cost and complexity, single point of failure, and privacy concerns.

User Experience and Adoption: Implementing MFA can introduce additional steps to the authentication process, potentially affecting user experience. Managing and remembering multiple authentication factors can be burdensome, especially if the factors are not user-friendly or require additional hardware. Balancing security and usability is essential to encourage widespread adoption.

Cost and Complexity: Implementing MFA systems may involve investments in hardware, software, and maintenance. Additionally, there needs to be an investment in education and training for the users. Organizations must consider the costs associated with deploying and managing MFA solutions, especially for larger user bases.

Single Point of Failure: While MFA adds an extra layer of security, it is not entirely foolproof. If one of the factors is compromised or the MFA system itself is vulnerable, the overall security can be compromised. Therefore, a comprehensive security strategy should be in place to address potential vulnerabilities not only at the initial implementation but throughout the lifecycle of the solution.

Privacy Concerns: Some MFA methods, such as biometrics, raise privacy concerns as they involve capturing and storing personal data. Organizations must ensure appropriate data protection measures and transparency to address these concerns. They must also consider local, state, and federal regulations associated with the use of biometric factors.

Considerations for Effective Implementation

The successful implementation of MFA requires careful consideration of various factors. Organizations need to assess their specific needs and risk profiles to determine the most appropriate combination of factors. Education and usability, compatibility and integration, and the lifecycle of the solution all need to be considered.

Risk Assessment and Tailored Approach: Organizations should conduct a thorough risk assessment to identify their specific security needs and determine the appropriate level of MFA implementation. Not all systems and applications require the same level of authentication. Making educated decisions based on risk will improve the success of an implementation.

Usability and User Education: Organizations should prioritize user experience and provide adequate training and education on MFA usage. Clear instructions, user-friendly interfaces, and guidance can help users understand the benefits and proper usage of MFA. Proper education will help to get buy-in from your organization and mitigate the risks of the users attempting to circumvent the controls altogether.

Integration and Compatibility: MFA systems should be integrated seamlessly with existing authentication systems and applications. Compatibility and interoperability should be considered to ensure smooth implementation without disrupting existing workflows. Improper integration can introduce additional risk and vulnerabilities to your organization.

Lifecycle Management: MFA systems should be regularly monitored and updated to address emerging threats and vulnerabilities. It is crucial to stay informed about new authentication technologies and best practices to maintain the effectiveness of MFA, as well as threats and vulnerabilities to the solution during the lifecycle of the solution.

Conclusion

While multi-factor authentication is not a panacea for all security challenges, it undoubtedly provides a robust and effective approach to secure access control. By combining multiple factors, MFA significantly reduces the risk of unauthorized access and strengthens the overall security posture. However, organizations must carefully consider the limitations, challenges, and implementation considerations to maximize the effectiveness of MFA. With proper planning, user education, and continuous monitoring, MFA can serve as a vital tool in protecting sensitive information and systems from unauthorized access in today's evolving threat landscape. AC

About the author

Antoinette King, PSP, DPPS, SICC, CMMC-RP is the founder of Credo Cyber Consulting, LLC, and has 21 years of experience in the security industry. Beginning her career as a field technician responsible for the installation, design, and implementation of integrated security solutions, Antoinette has worked on projects that include the protection of one of our nation's most treasured monuments, the Statue of Liberty. Antoinette has held roles within the security industry that include Engineered Systems Specialist, Operations Manager, Regional Sales Manager, and Key Account Manager in both integration and manufacturing. She recently joined iPro as a Director of Regional Sales East/ Head of Cyber Convergence.

Proud To Be On Just About Every Street In America

The past 75 years have seen us grow from a small manufacturer of garage door openers to one of the leading Access Control brands in America.

75th
1948 - 2023
DKS
DOORKING

Over the last seven decades, we've expanded from one building to a compound of seven (and counting), watched colleagues become loyal family, and cultivated strong supplier relationships that have become the backbone of the product we stand behind. As we've expanded our product line, we've been proud to become an integral part of our customers' lives at home, work, school, travel, and throughout their day as they move through America's doors and gates. We enter our 75th year of business with gratitude for our customers who have entrusted us to provide seamless Access Control they can count on. At DKS, we carry that trust with us as we look to the future, evolving Access Control to serve our customers better every day. Thank you for being with us.

Telephone Entry | Access Control | Gate Operators | Traffic Control

doorking.com/madeinusa
800-673-3299 • info@doorking.com

MADE IN USA

Member: AFA, DASMA, NAA, IDA, NPA, SIA, SSA, CANASA, NOMMA

Request information: www.securityinfowatch.com/10213482

To get more

www.stid-security.com

Request information: www.securityinfowatch.com/12266353

STid

UPGRADING YOUR SECURITY HAS NEVER BEEN EASIER

OBSOLETE TECH IS COSTLY

Up to 70% of organizations use access control technologies that are considered obsolete and no longer secure. Continuing to use these technologies means increased maintenance costs and difficulties in sourcing replacements. Even worse, older access control badges can be forged with equipment that is easily accessible online. You're risking serious security breaches, but what if you don't have the budget for a complete overhaul?

MIGRATE AT YOUR PACE

STid offers you the flexibility of moving at your own pace towards the highest levels of security. That's because our security readers, like the flagship Architect® series, are compatible with all access control cards, including 125 kHz, 13.56 MHz, NFC, and Bluetooth®. STid readers allow the use of obsolete card technologies while your organization gradually switches to higher levels of security. Once the migration is complete, deactivating older technology will be quick and easy.

THE SE8M MODULE

The Architect series includes seven interchangeable modules that can easily connect to a smart RFID and Bluetooth core. The SE8M module is a 125 kHZ Multi-Prox module which simplifies upgrades, technological migrations, and complex, multi-site configurations. It's compatible with many legacy Prox technologies, such as EM, HID Proximity, AWID, INDALA, IOPROX, and more. It can connect with standard, touchscreen, or keypad readers. The best part is that you can remove this module once you're done with your migration, and you won't have to reprogram the readers.

AWARD-WINNING

The Architect series is the most-awarded range of access control readers and just added another feather in its cap with the Electronic Security Expo's 2023 Innovation Award for Readers and Keypads.

STid strives to provide a more fluid and seamless access control process that is intuitive for its users without compromising on any security requirements. So, stop putting off that infrastructure

ESX
INNOVATION
AWARDS
2023WINNER

PHOTO: 1152853366 | KENTOH | GETTYIMAGES.COM

Does Interoperability Matter **When Integrating an Access Control System?**

The short answer is yes,but it is crucial to know why and where

by Lee Odess

It may be time to stop integrating and start interoperating.

The Proptech Advisory Board within the Security Industry Association recently collaborated with CREtech, a company with vast experience in proptech and commercial real estate, to produce The SIA Proptech Report. This report assessed proptech trends, market size, and purchasing interests related to security solutions in commercial real estate, including office environments and multi-family housing. The study involved surveying and interviewing many North American developers, owners, and operators.

When the topic of interoperability was raised, 83% of respondents believed that the current levels of interoperability between different security solutions were either fair (38%), poor (22%), or nonexistent (22%) - a staggering 83%. The question and responders' views were focused on broad security interoperability, not just access control. However, upon speaking to these developers, owners, and operators, you quickly realize that the majority view "security" as synonymous with "access control."

While they may be aware of our industry's focus on video, robotics, and much more, access control is a utility, and developers, owners, and operators view it as such. Access control helps secure buildings by keeping bad people out while enhancing the physical user experience for tenants, guests, visitors, and contractors. If a building had a voice, access control would be its mouth and vocal cords. It is front and center and top of mind.

And with that comes great responsibility and expectations on how it should show up.

Access control is an often underappreciated but crucial aspect of security. Beyond the technical capabilities, access control is the "distribution channel" for many other security products, including locks, readers, elevators, turnstiles, cards, fobs, video systems, alarms, and more. Access control systems are our industry's closest service to a "single pane of glass" for management, control, and data visualization. Although there are third-party platforms that aggregate access control data, access control systems on their own often play a critical interface role.

So, access control systems are the closest thing our industry and our customers have had to deliver interoperability in a very fragmented industry of parts and pieces.

However, upon closer examination of that sentence, things begin to fall apart.

And it is the "interoperability" part that falls short.

Interoperability between access control software companies and third-party locks, readers, elevators, turnstiles, cards, and fobs are rare. However, some lock companies are beginning to support other credential providers, and some reader companies are starting to support standards like OSDP. Additionally, some access control software companies support certain controller types like Mercury.

Let's not fool ourselves: what we have is more or less "integrated."

The Difference Between "Integrated" and "Interoperable"

Interoperable systems are capable of different systems working together smoothly, with attributes such as compatibility, scalability, flexibility, and adherence to standards. *Interoperability = seamless.*

On the other hand, **integrated systems** comprise separate components designed to work together. Still, they may not work smoothly with other systems or components outside the integrated system. *Integrated = works well with others.*

And here is the rub. The market wants interoperability, and our industry promotes and markets that we have it. However, we deliver something quite different but similar integration. Integration can frustrate and disappoint customers when they discover how our industry operates because as the customer pushes, we start to show the cracks in our systems.

Sure, we can tell how and why we do this as an industry, and when we do, we do it in the name of "safety and security." But the market is far more educated, aware, and has more options. And, if we were honest, we would also admit that we have been a cottage industry pushing proprietary systems. Our industry is what it is and sells this way because we know, and history has shown, that once you are locked into our system and install our hardware on the wall, it is rare for that product to be replaced.

The way we work is less about technical reasons and more about incentives. It is in our bones, our legacy, and how we have become experts in taking on the risk of keeping people and places so safe. But, again, those days are ending, and that is ok because, with all the technological advancements on the market now and coming soon, we can start to see how doing things differently may deliver better outcomes.

But is There Really a Downside to Us Being Integrated versus Interoperable?

The truth is that both integrated and interoperable systems have downsides.

Here are three examples of the downsides of integrated systems

- **Vendor Lock-In:** Integrated systems are often provided by a single manufacturer or a limited set of manufacturers, which can result in lock-in. Customers become heavily reliant on a specific manufacturer's technology and solutions, and switching to another system or manufacturer can be challenging and costly.
- **Lack of Flexibility:** Integrated systems are designed to work seamlessly within a specific ecosystem. However, they may need more flexibility to integrate

with external systems or adapt to changing business needs. Customization options may be limited, and components can be difficult to add or modify.

- **Limited Innovation:** Integrated systems may need to catch up in adopting new technologies or innovative solutions. These systems' development cycle can be slower than open or modular systems. Upgrades and new features depend on the manufacturer's roadmap, potentially limiting the ability to leverage emerging technologies or respond to market demands quickly.

While many pursue and push for interoperability, it is essential to note that it is not all upside. There are some downsides here as well to be aware of.

For example, there are four downsides to interoperability:

- **Complexity:** Interoperable systems often involve integrating multiple disparate components or technologies from different manufacturers. This complexity can make system implementation, configuration, and maintenance more challenging (especially long-term). Compatibility issues may occur due to differences in standards, protocols, or data formats, requiring additional effort to resolve.
- **Integration Costs:** Achieving interoperability typically involves additional costs, such as integration services, middleware (new to our industry and growing!), or custom development. Multiple manufacturers may charge for their products or services, and coordination among different parties may be required, leading to increased expenses.
- **Compatibility Risks:** Interoperability introduces the risk of compatibility issues. Updates, changes, or upgrades in one component may impact the compatibility of other integrated systems. Ensuring smooth interoperability can require ongoing monitoring, testing, and adjustments. This also means that investment to support interoperability is new and expensive.
- **Security Concerns:** Interoperability increases the attack surface for potential security vulnerabilities, especially cyber. Integrating systems from different manufacturers with varying security standards may introduce risks if adequate security measures are not implemented across all components.

It's crucial to consider security implications and adopt robust security practices when implementing interoperable systems.

So, Which is Better - Integrated or Interoperable?

Ultimately, the decision between interoperable and integrated systems should be based on a thorough evaluation of business requirements, existing infrastructure, budget, scalability needs, and the ability to manage complexity. Some organizations may prioritize flexibility and customization, favoring interoperable systems, while others may prioritize simplicity and quick deployment, leaning towards integrated systems.

> Customers want interoperability, mainstream markets expect it, and it is where our industry is headed.

Customers want interoperability, mainstream markets expect it, and it is where our industry is headed. The transition from integrated to interoperable will take time, and integration will not disappear. There will always be optionality and choice. However, interoperability will become the new norm, and those that get moving will benefit greatly. If not, once customers demand it and more companies from outside our industry start delivering on that demand, the legacy industry will be forced to comply. It's not a matter of if but when.

Something Else to Consider

The access control industry is changing and becoming more popular in a broader market. Its original purpose of keeping bad people out is being expanded to include allowing the right people in and providing additional value. As a result, the idea that it is the only way to integrate the various parts of the security industry is being challenged. More and more data aggregation, tenant experience, worktech, property management, point of sale, CRM, HR, ERP, and all Enterprise Software companies are seeing our nascent industry as an opportunity to combine with their core offering. This featurization of our industry is a massive threat.

We can summarize this evolution of the business as follows: *our product integrators (access control systems) are being integrated, and the resulting outcome is a value arbitration of our industry to someone else.*

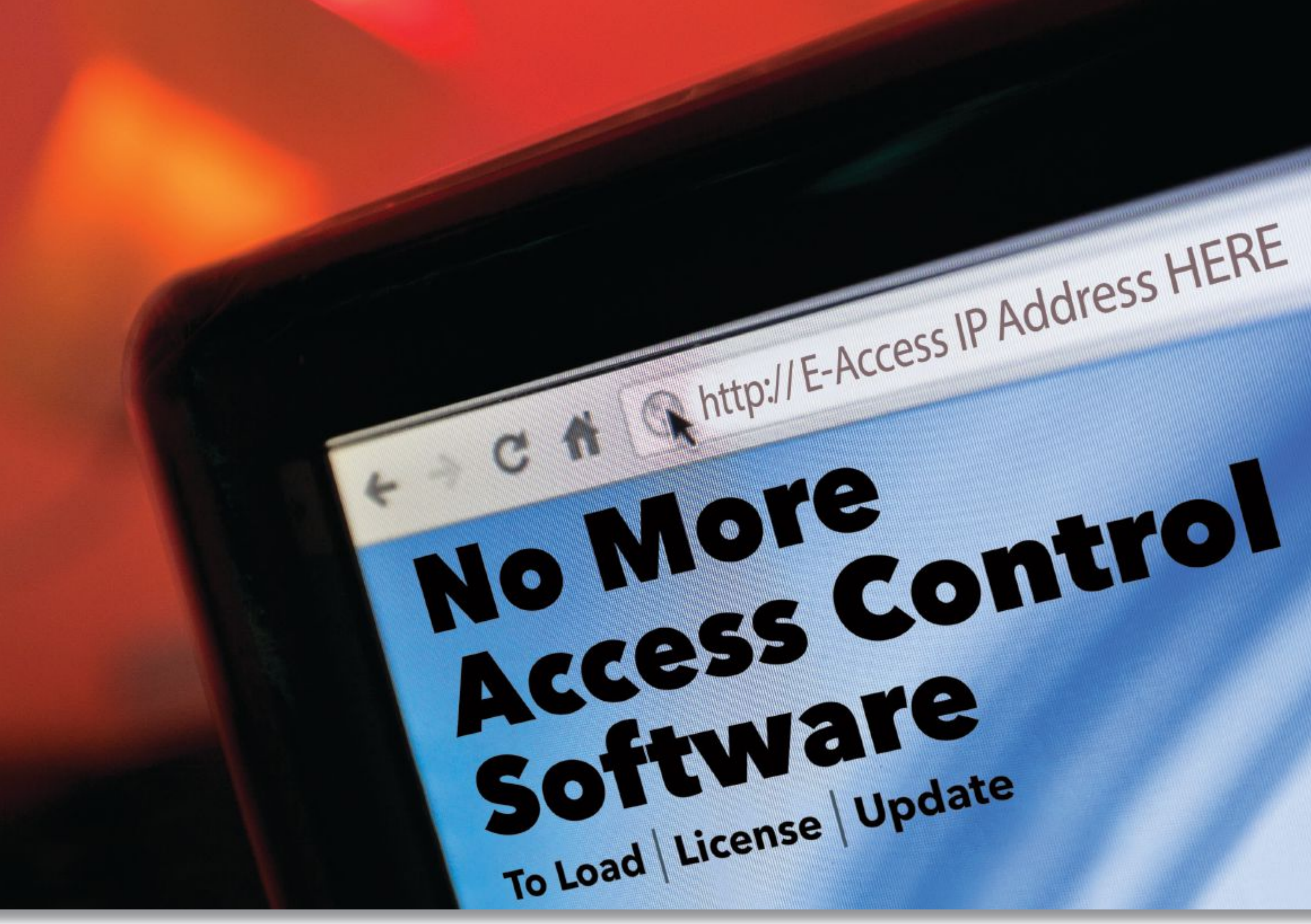
So, what should we do, and how do we participate in or at least attempt to slow this disruption down?

In short, we need to look seriously at how the access control industry views its core offering. As an industry, we must also clearly understand our views on what we value, what we are and are not willing to give up, and what other space we have permission to command, and be aggressive and unapologetic about it. And subsequently, we need to answer the question, is what got us here over the last 30 years going to be what is required for the next 30?

It may be time to stop integrating and start interoperating. The access control industry is an essential utility that delivers a value proposition many wish they had. Let's function as if. *AC*

About the author

Lee Odess is a globally renowned access control influencer, thought leader, consultant, speaker, and author who has spent his career reimagining the role of access technology in modern connected living experiences. Lee is a big believer that security goes beyond your front door and that true access means the enablement of spaces. Throughout his career, he has leveraged a number of platforms to help owners and operators adopt the latest technology to provide safe access, deliver innovative resident experiences and future-proof buildings. Lee is the independent go-to voice for the access control and smart lock industry. Email him at lee@leeodess.com or call 202-999-8180.



Smart Access Control Made Simple by Napco

Now there's no more software to load or update & super-fast setup, with new **E-Access® Embedded Self-Contained Controllers**. Web-browser-based access from anywhere; the Panel's IP address is the URL. Stop software hassles & additional costs*, while still getting all of the advanced features and flexibility you and accounts want: Cool App with dashboard and Free easy-issue Bluetooth mobile credentials; embedded Linux Operating System and 256 bit encryption; choice of slick readers (BLE, NFC, Prox, MiFare), easy configuration wizard, bulk ID uploads, Napco Gemini Security System integration and more. Simply scalable with choice of 1-, 2- or 4-Door Embedded Access Control Panels – for hundreds of doors and users.

Now Available at all Napco Distributors.
Ask about FREE Training Classes too.

* No charge after one-time cloud activation

NAPCO

1.800.645.9445
www.napcosecurity.com/products/e-access
Request information: www.securityinfowatch.com/10215125

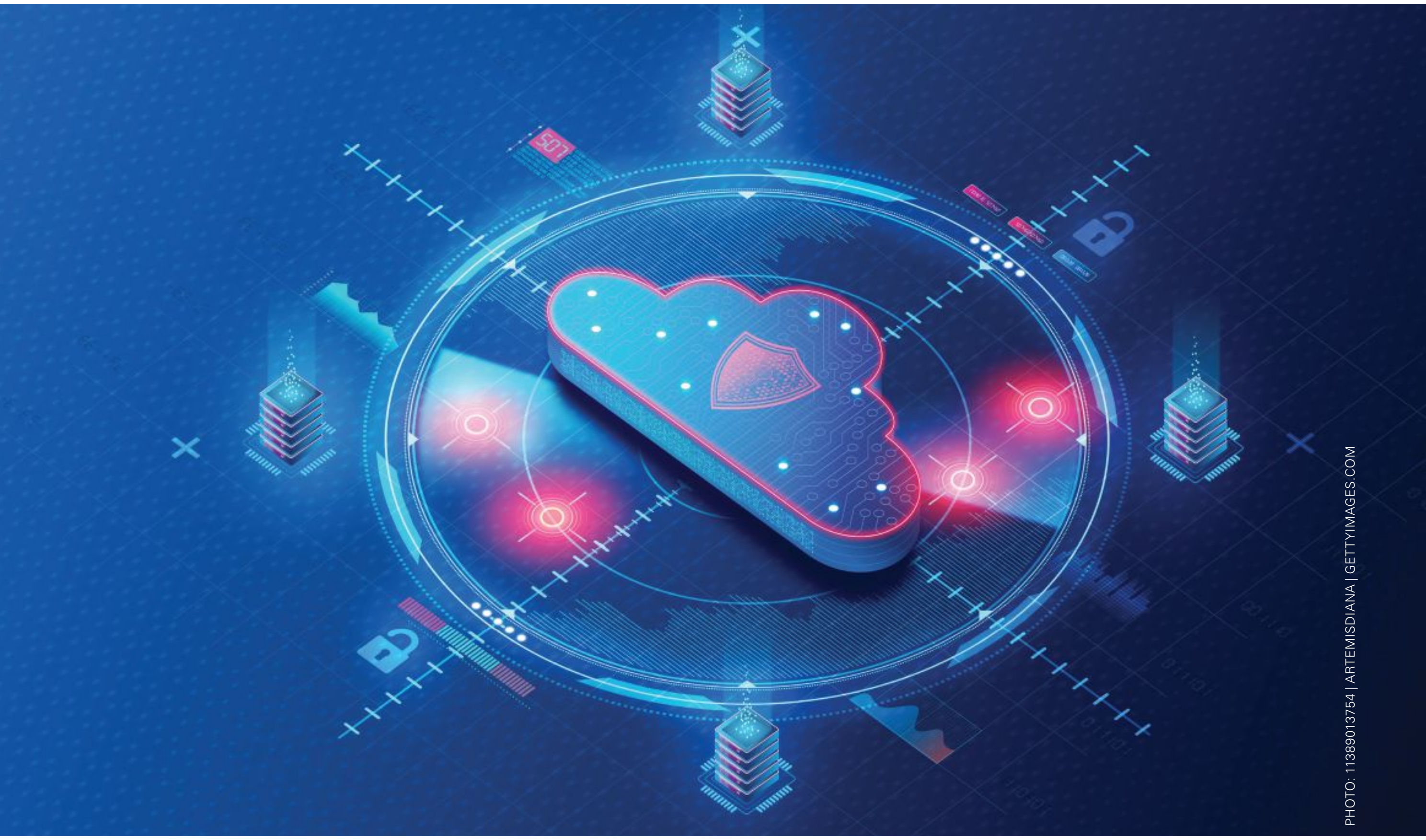


PHOTO: 1138901375 | ARTEMISDIANA | GETTYIMAGES.COM

How Cloud-Based Security **Ignites Digital Transformation**

by Scot Sturges

Access control and other security solutions have seen substantial growth over the last few years; the introduction of the cloud has dramatically impacted organizations in nearly every area: Business processes, data storage, conveyed workspaces, and security. While cloud-based access control has been slower to adopt in the United States, that is beginning to change. Meanwhile, other countries seem to be embracing it at a quicker rate. According to a recent investigation by Markets and Markets, cloud adoption will keep increasing and is expected to grow at a compound annual growth rate (CAGR) of 16.3% between 2021 and 2026.

The Benefits of Cloud-Based Access Control

Cloud-based access control can be a beneficial tool or service for any organization looking to track and manage its access control system, on-site or remotely. When associated with a surveillance system covering access points, a quality access control system confirms that only authorized personnel access the sensitive parts of any secure building. But what separates conventional access control systems from cloud-based access control systems? The significant difference is that while traditional access control systems are generally managed and operated on-site, cloud-based access control systems can be operated virtually anywhere via the cloud. In addition, numerous benefits present themselves to end-users and integrators.

A Straight forward Solution

Cloud-based applications are often considered user-friendly and straightforward to understand. With the mobility supplied by the cloud and flexibility with numerous platforms and devices, security team members with access to the system will presumably find the cloud-based applications preferable over the on-site alternative, given the possibilities for customization and simplicity for each available device. With an exclusively on-premise access control system, training can be prolonged, and more burdens are placed on the leaders of the security team. While most security teams can use on-prem systems appropriately, the cloud creates a streamlined, straightforward solution that safeguards the infrastructure and reduces human error.

Mobility and Flexibility

One of the primary advantages that cloud-based access control systems supply is mobility. With the ability to handle and manage systems via the cloud, users can do so almost anywhere utilizing an Internet connection and a mobile or net browser or app instead of an on-site location. In a post-Covid-19 landscape, this can be a practical ability to possess. The authority to grant and withdraw access from individuals - be it in the office or at home - makes the procedure more manageable for the security team and guarantees that sensitive materials are secured promptly after the loss of an employee. In addition, updating and sustaining the access control system is made easier on the cloud by supplying staff members with access to it remotely, allowing them to create modifications at any time. With standard access control systems, organizations often encounter problems with active key cards that need to be adequately deactivated, constructing potential risks and possible safety violations.

Cost- Effective

Cloud-based systems give companies the option of a lower total cost of ownership. Maintaining the system on the cloud offers numerous benefits compared to entirely on-premises systems. The cloud can save organizations money by offsetting the cost of data storage on-site, the price of powering extra hardware, and excessive on-site servers. Traditional on-premise systems are considered a CAPEX line item, and upfront investment is needed. A cloud-based solution is regarded as an OPEX purchase or operating expense that presents many advantages and ultimately depends on the package selected. By driving access control to the cloud, none of these costs that come with operating on-prem are present, and all of these costs are covered in one payment from your cloud provider.

> Cloud users can rest assured that their data is cyber-secure, and their system complies with the latest regulatory, security, and privacy regulations.

Data Redundancy

In the world of access control, possessing data is essential. It enables security teams to track who is permitted access to certain site areas and ensures that individuals are who they say they are. It also guarantees that data is protected in case of an emergency. For instance, power failures, workplace misfortunes, hardware and software malfunctions, and various other factors can generate valuable company data to become compromised. Nevertheless, this is only a matter of concern if the company's security data is stored on-premises.

With the cloud, users can rest assured that their data is cyber-secure, and their system complies with the latest regulatory, security, and privacy regulations. When an organization's access control data is stored in the cloud, they can rest easy knowing that the likelihood of catastrophic data loss is dramatically reduced due to the cloud's redundancy with off-premises data storage. This is not to imply that companies should not store data on-premises, but ensuring data redundancy makes for an ideal insurance approach.

Easy Integrations

Integrations make the world of access control go around. The ability to integrate other valuable, highly sought-after pieces of software quickly and effectively into your hardware or create a piece of software compatible with hardware from other companies is a trait that genuinely places high-quality organizations apart from the rest. Due to the character of the cloud, it is much easier to incorporate access control software into other systems, such as surveillance systems, intercoms, touch screens, and various other applications. As stated earlier, virtually any device with access to the Internet can be made to access the cloud, so it's no wonder that cloud-based access control integrations are quick and easy compared to conventional access control integrations. Just ensure your hardware is compatible with your cloud provider beforehand.

The Final Argument

If organizations are looking to adopt and evolve their security in the age of digital transformation and are wondering if cloud-based access control is necessary, it's paramount to ask this first: What types of organizations require access control? The answer to this question is essentially any organization with assets that need protection, conveying nearly all of them.

Suppose your organization has valuable assets that require monitoring and protection, such as heavy equipment, rare items, costly technology, sensitive materials, data, or any additional mission-critical assets. In that circumstance, your organization could profit significantly from a cloud-based access control system. Overall, cloud-based access control can be an ideal solution for almost every organization, and it can be as grand or small as you deem fit for your building, whatever the size and needs. *AC*

About the author

Scot Sturges is the Director of Business Development for ACRE North America and is based out of Addison, Texas. He is responsible for identifying new areas of growth and business opportunities for the ACRE portfolio brands. With over 14 years of experience, he is an integral part of the organization and continues to drive key client relationships.

Voice AI vs. Behavioral Biometrics

Examining the divide between technology and use case applications

by Raj Dasgupta

PHOTO: 284887105 | SKORZEWIAK | BIGSTOCK.COM

Beyond AI-generated voice profiles, fraudsters have many different ways to build up a physical biometric profile of a user.

Just last month, federal regulators at the FTC warned that "voice scams" are becoming more complex, targeted, and difficult to stop, due to an increasingly advanced process in which criminals "clone" a person's voice for nefarious purposes. These scams represent an evolution of traditional voice fraud– which relied on criminals impersonating law officers, bank officials, or loved ones in an attempt to persuade the victim to send over funds– typically through a payments platform or other service. While many organizations have adopted physical biometrics like voice confirmation to authorize payments (and lower losses), the advent of AI means that we're now seeing schemes that are increasingly targeted, advanced, and virtually undetectable by traditional security controls.

In the financial sector, specifically, audio-based schemes have become a boon for bad actors looking to defraud customers through impersonation and deceit. With AI-powered voice scams, criminals now have the ability to impersonate a loved one with a higher degree of accuracy, using a simple voice sample to replicate and then call someone requesting money. This new take on an old scheme has become significantly more effective and dangerous.

The most common targets of these attacks are older individuals who typically have lower rates of awareness and security literacy to identify and defend themselves against fraud. Recently, senior citizens in Canada lost up to $200,000 through AI-based voice scams. Even more alarming, criminals can also use stolen voice samples to try and bypass security protocols for a user's bank account, allowing them to freely move about and siphon funds. And, thanks to the rise of social media, there is no shortage of samples for criminals to choose from, leading to a new era where quite literally anyone could be impersonated and used for an attack.

With consumers concerned about protecting their privacy and maintaining security, it begs the question, what are the alternative controls that can be used to secure accounts and are not subject to being stolen or copied by cybercriminals? One solution lies in behavioral biometrics– a machine-learning-based technology that analyzes a user's digital, physical, and cognitive behavior to distinguish between cybercriminals/AI/bot activity and legitimate customers, weeding out the bad actors from the good. As a result, it's imperative to clear up misconceptions regarding behavioral biometrics and other tools that will be essential in defeating scams of the future.

> To understand why behavioral biometrics is essential, we must first understand why traditional safeguards have come up short.

What's the Difference?

To understand why behavioral biometrics is essential, we must first understand why traditional safeguards have come up short. Generative AI today is capable of making sophisticated copies of an individual's physical biometrics, like for example cloning their voice, which can now bypass previously effective methods of authentication.

Beyond AI-generated voice profiles, fraudsters have many different ways to build up a physical biometric profile of a user. They can scour social media and/or employ social engineering tactics to build up sophisticated copies of real photo IDs, simply steal a user's

The long-term ramifications of the generative AI technology rush may not be understood for some time...

PHOTO: 1462024468 | HIRUN | GETTYIMAGES.COM

smartphone or do a SIM swap to trick the system into letting them into the user's account. Particularly vulnerable to criminal exploitation are Photo ID scans. It's relatively easy to make a realistic copy of one's driver's license or passport and AI can trick even liveness detection systems. In each of these cases, a single breached access point can lead to the criminal accessing the system and then completing any number of illegal activities– most ending with a defrauded customer and the FI left to pick up the pieces.

Instead of relying on these traditional safeguards, FIs are better off establishing a risk-based authentication strategy whereby there is no single point of failure that can provide the fraudster access to the genuine user's account. Even if all the frontline defenses are breached, behavioral biometric intelligence can sniff out signs of risk, alerting fraud teams when subtle anomalies appear, even mid-session, between the user's genuine behavioral profile and the fraudster's AI-generated behavior.

This goes beyond simple voice commands or 2FA and instead uses factors that analyze not only user behavior but how well it matches up to criminal intent. For example, with this technology, it is possible to detect an ongoing scam in real time as the following elements can be picked up as irregular:

- Unusually long sessions and user hesitation when submitting a transaction, which could indicate coercion or intimidation.
- On mobile apps, an active voice call and movement of the voice from ear to mouth and then back again. Intermittent changes in the x,y, and z coordinates of the device also signal unusual user activity while being on their online banking account.
- On a desktop web login, aimless mouse motion is considered suspicious and a sign that the fraudster may need time to enchant, coerce and guide its victim. Or the victim needs to maintain the live session before an automated logoff stops a session or a screen saver takes over.

In other words, these systems are not simply relying on a single point of authentication to grant permission– say a voice-activated password– but instead continuously monitoring user behavior to detect anomalies based on past and present inputs. This is in addition to verifying the traditional controls such as location, device fingerprint, and IP address. Behavioral biometrics is not only capable of identifying hacked accounts but also ascertaining when the genuine account owner is acting under duress or being coached by a criminal.

Where Do We Go?

The long-term ramifications of the generative AI technology rush may not be understood for some time. Still, it seems safe to say that operating under true privacy will be, if not already, elusive. It is important for financial organizations to install safeguards that don't rely on information that can be copied, including physical biometrics like voice verification. All entities entrusted with safeguarding consumer privacy will need to have a multi-tiered risk-based authentication approach and institute a rapid response system to ensure that their customers' data is always secure. Behavioral biometrics will fill this need, and crucially, do so without requiring any additional steps on the user's part– making it a seamless, effective, and powerful counter to emerging AI cyber threats. As awareness and adoption of these tools become more commonplace, we'll also see an increased willingness from consumers to use these services, and significant progress made in the fight against fraudsters. *AC*

About the author

Raj Dasgupta is Senior Director, Global Advisory at BioCatch with over 15 years of Financial Services industry experience in the U.S. has worked for HSBC, Yodlee, Intuit, ID Analytics and TransUnion prior to joining BioCatch. Throughout his career, he has been at the cusp of business and technology advising his customers on how technological solutions can be operationalized to solve real-life business problems

CAMDEN
CAMDEN

How to Create a Seamlessly Effective **Video and Access Control System**

Integrating access control with video surveillance requires a thoughtful approach to data protection and privacy

by Darnell Washington, CISSP

PHOTO: 1174652880 | ISMAGILOV | GETTYIMAGES.COM

In today's security-conscious world, organizations of all sizes are increasingly recognizing the importance of implementing robust security measures. Two essential components of a comprehensive security system are access control and video surveillance. By integrating these two systems, organizations can enhance their security posture and improve their ability to prevent, detect, and respond to potential threats. With evolving information published and available to defeat these systems (YouTube, google, and a variety of web platforms) countermeasures and best practices must be continually developed and improved for integrating access control with video surveillance to deploy the most effective security solution.

Many solutions, whether wired or wireless, have specific pros and cons and it is essential to obtain adequate information on your environment. You must consider where you are deploying your video and access control systems to make the best decisions relative to the cost of implementation and desired benefits, etc. One key decision that needs to be made is the type of centralized management platform you choose. Milestone, Genetec, Bosch, and larger integrators like Johnson Controls and HID offer enterprise multi-vendor products that integrate video and access control systems seamlessly.

Whatever platform you choose, it should provide a unified interface for monitoring and managing both your access control and surveillance systems, enabling security personnel to view live and recorded video feeds alongside access control events. By having a centralized management platform, your organizations can streamline security operations, reduce response times, and gain a holistic view of your physical security environment.

You can also train systems to detect piggybacking, object left, and data analytics that can detect anomalies and deviations of normal activities with your environment. Don't forget that cybersecurity vulnerabilities must be addressed during this phase and ongoing testing and certification of the systems to ensure exploitation by unauthorized users are mitigated.

Environmental Factors When Considering Access Control and Video Solutions

Regardless of which solution you use, it is important to consider the constraints of your surveillance and access control needs when choosing between wired and wireless solutions. Factors such as the size of the area, desired coverage, security considerations, and budget will help determine the most suitable option for your situation.

The benefits of wired solutions are reliability, security, consistent performance, and power requirements. Wired systems generally provide a more reliable connection compared to wireless solutions. They are not susceptible to signal interference or interruptions caused by obstacles such as walls or other wireless devices. They are also more secure as they are less prone to hacking or unauthorized access, as they do not rely on wireless signals that can be intercepted. This makes them a preferred choice for sensitive areas where security is paramount. Wired systems also perform more consistently since they are not affected by fluctuations in wireless signal strength. This is crucial for applications that require real-time monitoring and high-quality video transmission. Wired systems can also draw power directly from the electrical grid, or Power over Ethernet (POE), eliminating the need for batteries or charging. This ensures continuous operation and eliminates the risk of power loss.

Wireless solutions are gaining ground, almost comparable to wired systems due to technological advancements (especially in cyber and logical security). Most of the benefits derived from wireless solutions include flexibility and scalability, mobility, and ease of integration with IOT/OT systems. When deploying wireless solutions in challenging places wireless systems can be expanded or relocated inexpensively if an access control setup or configuration change is required. Additionally, wireless systems can integrate with other devices, enabling advanced features and automation. For example, wireless access control systems can be integrated with smart locks, enabling remote control and management of access permissions.

Deploying a Secure Cybersecurity Framework to Your Platform

When integrating access control you should also consider implementing role-based access and privileges for video surveillance. Different security personnel may have varying responsibilities and levels of authorization when it comes to accessing video feeds. By defining specific roles and privileges within the system, organizations can ensure that only authorized individuals can view or retrieve specific video footage. This approach helps maintain data privacy, prevents unauthorized access, and reduces the risk of misuse or tampering. It is recommended that Smart Cards be required as multi-factor identity verification for System Administrator and Audit functions.

Integrating access control with video surveillance requires a thoughtful approach to data protection and privacy. Organizations must comply with relevant regulations and standards governing the collection, storage, and use of personal data captured by video surveillance systems. It is crucial to establish clear policies and procedures that secure the handling and retention of video footage and limit access to authorized personnel only. Implementing encryption, secure storage, and regular data backups are also essential practices to protect sensitive information.

AI-Based Analytics and Alerts

Using Artificial Intelligence (AI) based intelligent analytics and alerts is another great best practice for integrating seamless video and access control systems. Advanced video analytics can automatically analyze video feeds and detect unusual or predefined events, such as unauthorized access attempts or loitering. When such events are identified, the system can generate real-time alerts to notify security personnel.

Integrating these analytics with access control data enables a more proactive security approach, helping to prevent incidents before they escalate. Training analytics is not always an easy task, but the more work that is done up front makes the entire process easier.

Creating an effective Video and Access Control system is not possible without a comprehensive log and audit system.

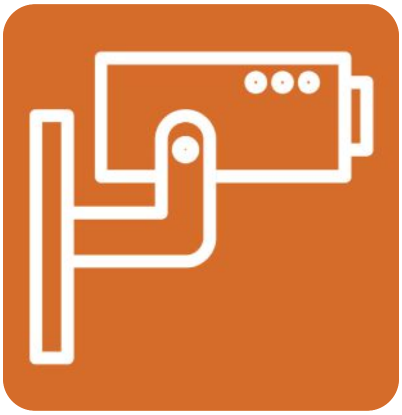
Seamlessly integrating advanced video analytics can analyze video footage in real-time or post-event to detect and identify objects, people, behaviors, and events. This includes features like object detection, facial recognition, license plate recognition, intrusion detection, people counting, and crowd detection. This analytics help in generating alerts based on specific criteria, such as detecting unauthorized access, loitering, or unusual behavior. A one size fits all approach never fits this scenario when creating an effective video and access control system.

Video and Access Control Analytics focuses on analyzing data to identify patterns, anomalies, and potential security risks. This may involve monitoring access logs, user behavior, access attempts, and access patterns to detect suspicious activities or policy violations. Using Artificial Intelligence (AI) analytics in access control systems can generate alerts for predictive or actual events like multiple failed access attempts, access outside of authorized hours, or attempts to gain access with invalid credentials.

Behavior analytics leverage machine learning and AI algorithms to analyze patterns of behavior within access control and video surveillance systems. This can include identifying normal behavioral patterns and detecting anomalies that may indicate potential security threats. For example, unusual movements, loitering in restricted areas, or repeated access attempts can trigger alerts for further investigation.

Event correlation involves integrating data from various sources, such as access control events, video surveillance footage, alarm systems, and other sensors. By correlating events across multiple systems, it becomes possible to identify complex relationships and trigger alerts based on specific combinations of events. For instance, if an access control event coincides with a specific video surveillance event, it may warrant immediate attention and generate an alert.

Predictive AI and/or Real-time alerting ensures that security personnel is notified immediately when a security event or anomaly occurs or has the potential of occurring. Alerts can be delivered through various channels such as email, SMS, push notifications, or integration with centralized security management platforms. The ability to customize and prioritize alerts based on severity and context is crucial for effective incident response.



A Hotkey should be enabled to enable the operator to flag a suspicious event or alert for further review, and logs should be maintained for a minimum of three months to correlate potential events to suspicious activity. Quite often logs are not reviewed by humans on a periodic basis, leading to security failures and loss.

AI-based Intelligent dashboards provide a visual representation of analytics results, key performance indicators (KPIs), and security metrics. These dashboards enable security operators to monitor and analyze data effectively, identify trends, and respond proactively to security incidents. Reporting capabilities allow for historical analysis, performance evaluation, and compliance auditing.

Tying it All Together- Logs and Audit Systems

Creating an effective Video and Access Control system is not possible without a comprehensive log and audit system. Access control and Event logs can be generated from various sources, including physical security systems (such as surveillance cameras, access control systems, and alarm systems), network devices (like firewalls, routers, and switches), servers, applications, and user activity tracking mechanisms. These logs not only provide assurance that the systems are working properly, but they also serve as valuable sources of information for incident response, forensic investigations, compliance audits, and continuous monitoring of security measures.

These types of logs capture diverse aspects of security events. Physical security, logs may include video footage, access control records, and sensor data. Cybersecurity logs can include system logs (such as Windows Event Logs or Syslogs), application logs, firewall logs, intrusion detection system (IDS) logs, antivirus logs, and more. Logs must be protected against cyber threats and unintentional deletion one of the first things cyber attackers seek to do is to delete control and event logs to hide their tracks.

By synchronizing and correlating these event and audit logs from video and access control systems you will effectively enhance incident response capabilities, strengthen security measures, and mitigate future risks. The ability to monitor event logs provides a historical record of events, enabling security teams to identify patterns and detect deviations and anomalies – including internal threats from inside your organization.

Linking events from synchronized systems reduces the substantial effort required to piecemeal relevant artifacts together in the event of an incident. Video and access control events, such as card swipes or door unlocks, should be capable of tying corresponding video footage within specific time intervals.

When an access control event occurs, the associated video feed should automatically display on the monitoring screen, providing real-time visual verification of the event. This correlation helps security personnel quickly identify any potential security breaches or suspicious activities, allowing them to take immediate action.

The system logs should be regularly reviewed and evaluated for log content, and log management to enable searching to identify anomalies and deviations and retained for a period required by regulatory agencies or corporate policy.

> A tailored approach is recommended when implementing an integrated access control and video surveillance solution.

Conclusion

It is important to remember that each organization's security requirements may differ, so a tailored approach is recommended when implementing an integrated access control and video surveillance solution. While no system is flawless integrating a seamless video and access control system on a single framework can be a powerful way to cost-effectively enhance security measures and mitigate potential risks. By evaluating the environmental factors, and following cybersecurity standards to prevent security breaches, and deploying intelligent AI-based alerts to system logs, and synchronizing the data --operators can easily make determinations and quick responses to incidents and /or threats quickly and effectively.

About the author

Darnell Washington, CISSP, is the President of SecureXperts. He is an industry-recognized thought leader, educator, public speaker, and entrepreneur specializing in the development, design, and implementation of commercial and industrial technologies in cybersecurity, systems automation, and critical manufacturing. He has developed leading-edge technology for international defense, government, aerospace, commercial and public/private sectors.

Access Chaos is More Than a Cryptic Buzzword

For 50 years we have had to live with physical access control systems that were not manageable at any large scale.

by Ray Bernard, PSP, CHS-III

PHOTO: 1462024468 | HIRUN | GETTYIMAGES.COM

When I first heard the term Access Chaos, I thought it was likely to be a marketing term of little practical use. Digging deeper, I learned that it is being used to describe a 50-year-old situation: that physical access control privileges are less and less manageable as two things grow in size: the number of electronically controlled doors or gates, and the number of access cards or credential holders in the system.

Recently I heard one particular company's story. They have 25,000 employees. Every year 2,000 individuals exit the company, 2,500 are hired to backfill empty positions or fill new ones, 800 change roles or working locations, 1,000 are added due to acquisitions, and another 500 left due to subsidiary sell-offs. On average, 25% of all people's records change every year. That's 6,250 personnel changes.

They believe it likely that hundreds of their people have inappropriate access resulting from a variety of human mistakes, many of which are bound to relate to critical asset areas.

Traditional physical security systems rely on relational databases for their data storage.

Any of the access privilege errors can result in multiple access violations. But because the changes are ongoing, they don't have any practical way of knowing where the errors are.

Furthermore, some percentage of the access privilege errors are cumulative, meaning that they are not solved by people leaving the company. *Thus, incorrect access liability grows each year, and the organization is increasingly subject to the very threats the access control system was designed to prevent.*

This is the situation that RightCrowd **(www.RightCrowd.com)** has accurately labeled "Access Chaos." Per my own observations over the years, it exists with most employee populations that have over 1,000 access privilege holders. The larger the employee population, the greater the number of cardholders with unintended access privileges to critical asset areas.

In addition to access errors within the access control system itself, there are also other access control factors that are managed manually, and often serious corporate liabilities exist because of human errors in their management. Two of them are insurance and training requirements.

For personnel safety and other reasons, access to hazardous operations areas requires individual safety training. Additionally, contractors working on-site often have insurance coverage requirements. A serious or fatal on-the-job accident caused by an untrained person or an uninsured person can result in a multi-million-dollar settlement, not to mention the business interruption and the demoralizing effect on workers in the operations area.

Fortune 500 Companies

Only a small percentage of Fortune 500 companies have company-wide identity management systems and dedicated people who perform oversight on the access chaos factors. But most large business organizations just can't dedicate personnel to the task and aren't really aware of the true risks involved.

But this has always been the case. So why create the label now?

Access Analytics

RightCrowd has introduced a new cloud application that the company says, once and for all, lets you put an end to access chaos.

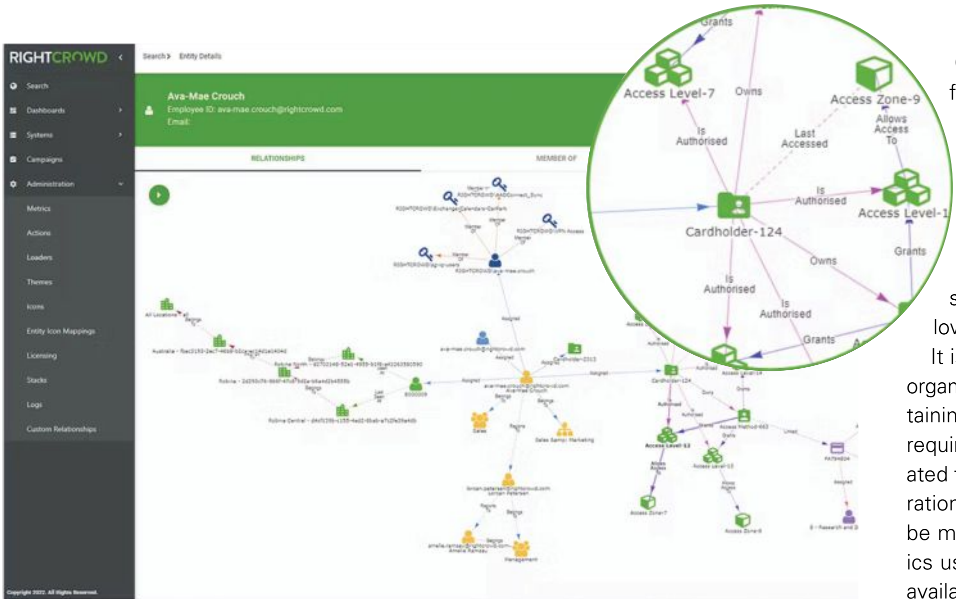
Called *Access Analytics*, it allows physical security, OT teams, IT, HR and business personnel to collaborate, review and take action to correct inappropriate physical or logical access to any assets and enterprise systems using a single graphical view that can present the access privilege information from multiple perspectives.

It can answer simple questions like, "Whose safety training is expiring within the next 30 days?" Access Analytics can initiate a notification to the individuals who need to redo their training, the people who manage their access privileges, and the supervisors who may need to help facilitate the time off work for training.

Why hasn't anyone done this before? Well, it simply wasn't possible using the database technologies that have been available – until now.

Access Analytics is a lightweight software that works with daily input feeds, typically a simple CSV file exported from the systems with access privilege information.

It puts the data into a *graph database*, a new type of database that can be used to store information about people and assets and the requirements and relationships that relate to them. A graph database is a special kind of database built to hold and navigate billions of relationships and query them with millisecond latency.



RIGHTCROWD

- Search
- Dashboards
- Systems
- Campaigns
- Administration
  - Metrics
  - Actions
  - Loaders
  - Themes
  - Icons
  - Entity Icon Mappings
  - Licensing
  - Stacks
  - Logs
  - Custom Relationships

Search > Entity Details

Ava-Mae Crouch
Employee ID: ava-mae.crouch@rightcrowd.com
Email:

RELATIONSHIPS | MEMBER OF

Copyright 2022. All Rights Reserved.

Figure 1. View of particular cardholders' access-privilege-related data

PHOTO: RIGHTCROWD.COM

The Profium website describes the two following graph database use cases.

How is it possible that LinkedIn can show all your 1st-, 2nd-, and 3rd-degree connections, and the mutual contacts with your 2nd-level contacts, all in real-time? It's because LinkedIn organizes its entire contact network of 660+ million users using a graph database. Netflix uses a graph database for its Digital Asset Management (DAM) because it is a perfect way to track which movies (assets) each viewer has already watched, and which movies they are allowed to watch (access management). Note also that Identity and Access Management (IAM) has an essential role in DAM.

Traditional physical security systems rely on relational databases for their data storage. Relational databases aren't designed to manage the scale and complexity required for the kinds of multi-faceted access control that large organizations need.

The graph database, plus RightCrowd's patented way of using it, is what makes the performance of Access Analytics possible.

Access Analytics works with any access privilege management software, including traditional physical access control systems, Microsoft Active Directory, visitor management systems, parking access management systems, physical lock and key management software, HR systems, learning management systems and so on. It works for physical card credentials of all types, as well as mobile device digital credentials. The application is future-proof in the sense that it can work with all the systems and credentials in place now, plus those that will be adopted in the future.

You can also include logical access as well. For example, people who have access to a physical security system VPN.

Using Access Analytics

Access Analytics is a tool that uses your existing access management roles, responsibilities, processes and procedures to correct access privilege errors.

It does this by providing notifications to the access decision-makers, who can use the Access Analytics main view **(see Figure 1.)** to see the full context for the recommendation if needed.

Often there is no need to consult the full view, because the rationale behind the recommendation is obvious, such as to remove a cardholder because the person's employment was terminated, as shown in **Figure 2.**

There are no automatic access changes made to any access control systems or databases, thus it is a very low-risk deployment.

It is also future-proof because when an organization adds or removes a system containing access privilege information, it only requires a new CSV file data feed to be created for the addition and a simple configuration change in Access Analytics that can be made by an authorized Access Analytics user. (There are other data feed types available. The CSV file is the simplest one and is most commonly used.)

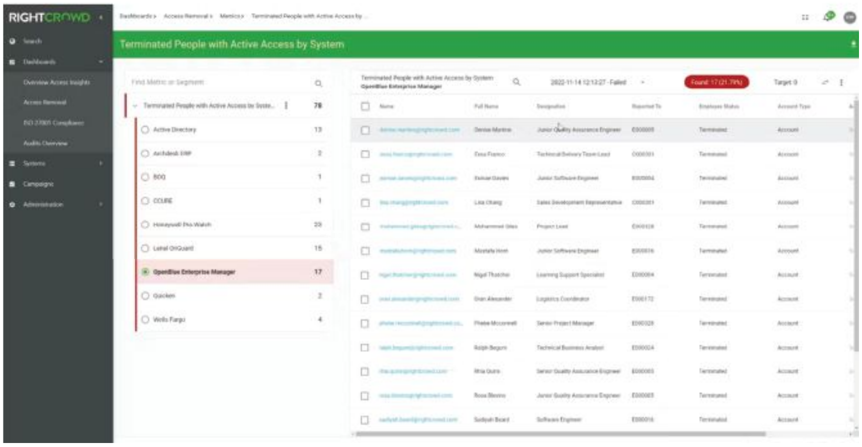
Self-Paced Adoption

Access Analytics can be deployed one site at a time, beginning with the highest- headcount sites (the highest risk of access privilege errors) and moving on from there. It establishes immediate visibility into the current state of access privileges, which can be viewed by the facility, access control system, or privilege holders.

It can also consider the future state, such as access privilege requirements that are about to expire, as exist for licenses, insurance, training and certifications.

Rules

An important feature of Access Analytics is its use of rules. Access Analytics provides a set of default rules, for example,



RIGHTCROWD

- Search
- Dashboards
  - Overview Access Insights
  - Access Removal
  - ISO 27001 Compliance
  - Audits Overview
- Systems
- Campaigns
- Administration

Dashboards > Access Removal > Metrics > Terminated People with Active Access by ...

Terminated People with Active Access by System

Find Metric or Segment

Terminated People with Active Access by Syste...	78
○ Active Directory	13
○ Archdesk ERP	2
○ BOQ	1
○ CCURE	1
○ Honeywell Pro-Watch	23
○ Lenel OnGuard	15
● OpenBlue Enterprise Manager	17
○ Quicken	2
○ Wells Fargo	4

Terminated People with Active Access by System
OpenBlue Enterprise Manager

2022-11-14 12:13:27 - Failed

Found: 17 (21.79%)

Target: 0

□	Name	Full Name	Designation	Reported To	Employee Status	Account Type
□	[illegible]	Denise Martins	Junior Quality Assurance Engineer	E000005	Terminated	Account
□	[illegible]	Essa Franco	Technical Delivery Team Lead	C000301	Terminated	Account
□	[illegible]	Eskuar Davies	Junior Software Engineer	E000004	Terminated	Account
□	[illegible]	Lisa Chang	Sales Development Representative	C000301	Terminated	Account
□	[illegible]	Mohammed Giles	Project Lead	E000128	Terminated	Account
□	[illegible]	Mostafa Hani	Junior Software Engineer	E000016	Terminated	Account
□	[illegible]	Nigel Thatcher	Learning Support Specialist	E000064	Terminated	Account
□	[illegible]	Oran Alexander	Logistics Coordinator	E000172	Terminated	Account
□	[illegible]	Phebe Mcconnell	Senior Project Manager	E000028	Terminated	Account
□	[illegible]	Ralph Begum	Technical Business Analyst	E000024	Terminated	Account
□	[illegible]	Mia Quinn	Senior Quality Assurance Engineer	E000003	Terminated	Account
□	[illegible]	Rosa Blevins	Junior Quality Assurance Engineer	E000003	Terminated	Account
□	[illegible]	Sadiyah Beard	Software Engineer	E000016	Terminated	Account

Figure 2. List of terminated people who still have access privileges

PHOTO: RIGHTCROWD.COM

BEST EHD9000 Closer

dormakaba Lyazon with Saffire EVO Lock

Alvarado Argus V60 Compact Optical Turnstile that terminated people should not have access privileges. Users can add custom rules, defining, for instance, that people on a leave of absence should have their access privileges suspended.

Once a few sites or access control systems have been enrolled in Access Analytics, and any important custom rules have been established, enrollment of additional sites can be accomplished in sequence or in parallel – at whatever pace is non-burdensome.

> Using Access Analytics to resolve the access chaos problem prior to large-scale upgrades will lower the cost and shorten the timeframe of the upgrade.

Auditability

A key shortcoming of physical access control systems has been the lack of auditability regarding access privileges. Even for companies who have very specific access control policies and procedures for physical access management, auditing conformance to those requirements has not been possible.

Additionally, Access Analytics eliminates manual access management processes as single points of failure in access management. Incorporating it as part of the physical access control system deployment provides daily automated assurance against manual errors and process incomplete workflows (such as can happen with vacations, transfers, travel, etc.).

Physical Access Control System Upgrades

Many companies are currently considering upgrading multiple disparate physical access control systems to standardize on a single access management software product. Sometimes that upgrade is software-based, such as for deployments based on Mercury Security hardware, and sometimes it involves hardware as well.

Any such deployment project can be simplified by performing access-privilege cleanup prior to performing the upgrade. Historically, some companies have decided to fix their access chaos problem by re-credentialing all individuals and starting from scratch with the assignment of access privileges. That approach is highly disruptive, always takes longer than estimated, and doesn't keep access chaos from creeping in again, which is what always happens.

Other companies have simply exported the cardholder and privilege data from their existing access control systems and imported it into the new system. This preserves the access chaos without providing a means to correct it.

Companies take this approach when they don't realize the full extent of their

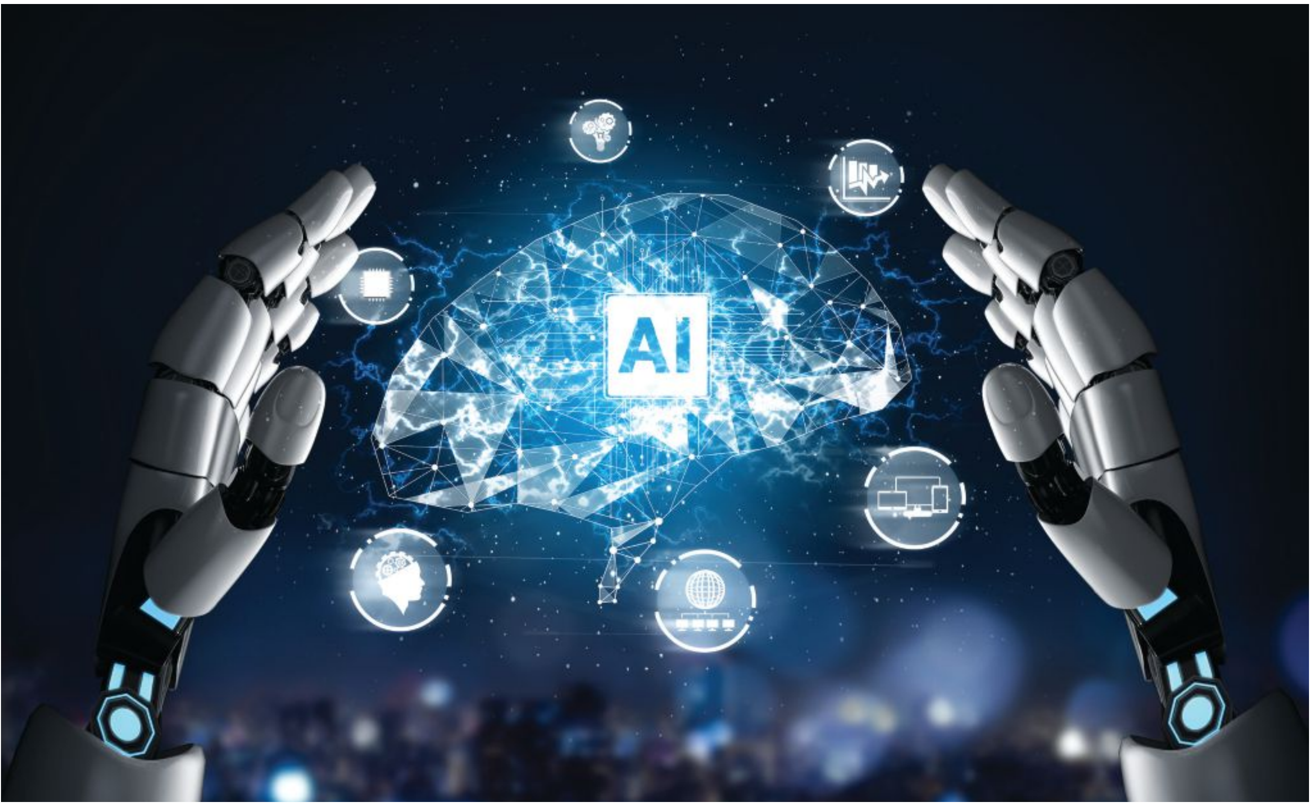


PHOTO: 1245974261 | BLUE PLANET STUDIO | GETTYIMAGES.COM access chaos and wrongly assume that somehow the new system will let them manage access privileges better.

Using Access Analytics to resolve the access chaos problem prior to large-scale upgrades will lower the cost and shorten the timeframe of the upgrade. It will enable progressive upgrades at any pace that makes sense, and ensure that access privileges are always correct throughout the upgrade.

There will be no "limbo" state for access privileges where no one is sure where access privileges stand until the upgrade is complete. This can be critically important for organizations with regulatory requirements relating to physical access control.

Knowing vs. Assuming

For the first time in the history of physical access control, it's possible to know the exact state of access privileges. This writer has been involved in several dozen large-scale access control upgrade projects. In every case, the state of access control privileges was always much worse than anyone had thought. Unraveling the mess always impacted project execution time.

This article is not a full description of the Access Analytics product. It has only scratched the surface of its features and the extent of its application. The main points are these. For the first time in the 50-year history of physical access control systems, physical access privileges can be managed fully and accurately, and in a non-burdensome way – for any sizeable access control system deployment, no matter how many brands of access control systems there are, and regardless of the number of sites. Until now, the technology did not exist (modern graph databases and cloud computing) that could handle the management of the complex factors involved in truly comprehensive access management.

There are other factors, such as the cyber strength of access credentials, tailgating, and the trend toward open-space building floor plans. However, addressing those factors is practically meaningless if there is no tight control on access privileges. *AC*

About the author

Ray Bernard, PSP CHS-III, is the principal consultant for Ray Bernard Consulting Services (RBCS), a firm that provides security consulting services for public and private facilities **(www.go-rbcs.com)**In 2018 IFSEC Global listed Ray as #12 in the world's Top 30 Security Thought Leaders. He is the author of the Elsevier book Security Technology Convergence Insights available on Amazon. Follow Ray on Twitter: @RayBernardRBCS.

Tips on Automatic Door Controls and Restroom **Code Compliance Applications**

Building codes continually evolve so it is incumbent that security practitioners stay current

by SecurityInfoWatch.com Staff

Applications for access control are wide and varied. Countess enterprises across all industry sectors have adapted varying access control technologies and capabilities to meet their site-specific needs and requirements. Together with their systems integrations partners, stakeholders can determine the access measures that are best tailored to their individual facilities.

However, when it comes to automatic door control and code compliance in restroom applications, the requirements are typically spelled out very clearly and in no uncertain terms. The Ontario Building Code (OBC), which went into effect on January 1, 2015, for example, mandated the installation of emergency call systems in barrier-free and universal washrooms. Although the code requirements were originally only applicable to the province of Ontario, Canada, they continue to serve as a model for emerging code requirements for emergency call systems in universal washrooms across North America.

Codes & Standard — What You Need to Know

Barrier-free access to buildings and restroom facilities is mandated across North America by state or provincial building codes. In the U.S., barrier-free access is also mandated by federal law but allows interpretation and enforcement to be determined by each individual state.

In Canada on the other hand, the National Building Code provides a model building code that is used where no provincial code is adopted and also forms the basis for all provincial building codes. The result of these vastly different approaches is that the Canadian requirements for automatic doors on restrooms are uniform whereas the American requirements can vary markedly from state to state. Both end users and systems integrators should refer to the specific building codes that apply in their particular state.

There is one common objective, however, and that is to provide high visibility and enhanced user convenience in ADA-compliant automatic door applications. Therefore, having a solid understanding of The Americans with Disabilities Act (ADA) is so important.

Restroom control kits should provide a complete solution that includes 'Push/Wave to Open' and 'Push/Wave to Lock' activation switches, a 2 Amp. power supply and controller in a small metal cabinet, 'universal' electric strike, and door contacts.

PHOTO: COURTESY OF CAMDEN

The Americans with Disabilities Act (ADA)

A federal law, ADA, is designed to provide equal access for all citizens. All buildings that are open to the public are required to provide equal access for people with disabilities. All visitors and occupants must be able to safely enter and exit the building and move throughout the building without obstruction. There are two key technical regulations that inform the Americans with Disability Act. These are the ADA Accessibility Guidelines (ADAAG) and the Uniform Federal Accessibility Standard (UFAS). Both the ADAAG and UFAS are based in large part on the technical criteria that is specified in the national voluntary consensus standard, ANSI A117.1

AHS

ACCESS HARDWARE SUPPLY

STARRING

ASSA ABLOY
Opening Solutions

Adams Rite ASSA ABLOY · h.e.s. ASSA ABLOY · SARGENT ASSA ABLOY · SECURITRON ASSA ABLOY · NORTON RIXSON ASSA ABLOY · Corbin Russwin ASSA ABLOY

NORTHERN CA ★ 14447 GRIFFITH STREET, SAN LEANDRO, CA 94577

SOUTHERN CA ★ 10824 EDISON COURT, RANCHO CUCAMONGA, CA, 91730

IP INDUSTRY PROFESSIONALS
ALL AGES ADMITTED

NOW PLAYING

(800)348-2263
www.accesshardware.com

Request information: www.securityinfowatch.com/10722906

Understanding ANSI Standards

The American National Standard Institute (ANSI) is a private, nonprofit membership organization that provides a voluntary system for the development of standards, including those applicable to the installation of automatic doors.

There are two ANSI standards that are commonly cited by both U.S. and Canadian building codes in regard to automatic doors in restrooms: ANSI A117.1 is the standard for Buildings and Facilities - Providing Accessibility and Usability for Physically Disabled People, and ANSI A156.19, which is the standard for Power Assist and Low Energy Power Operated Doors.

Restroom control privacy systems are comprised of various system components and are designed to keep in compliance with applicable codes and requirements.

Building Codes

Because each U.S. state has the authority to interpret federal ADA requirements and to legislate those requirements as law as they see fit, many states have different approaches to accessibility regulations. Some states have adopted ANSI A117.1, the UFAS, ADAAG or model building codes (such as the International Building Code or Universal Building Code), all of which are relatively similar. Another group of states relies on one or another of those sources as a basis for their regulations but have other requirements and do not reference them by name.

- A third and smaller group of states have legislated their own unique standard and code requirements. In addition to these building codes, there are others that your restroom project may need to comply with. The NFPA National Fire Code or International Fire Code is of particular importance, and because restroom doors are egress doors, compliance will be required by the local AHJ.

Types of Systems

Restroom control privacy systems are comprised of various system components and are designed to keep in compliance with applicable codes and requirements. They represent a growing segment of the access control market as the industry is experiencing rapid growth in the installation of automatic operators on restroom doors, as well as in a wider scope of building occupancies. Restroom control kits should provide a complete solution that includes 'Push/Wave to Open' and 'Push/Wave to Lock' activation switches, a 2 Amp. power supply and controller in a small metal cabinet, 'universal' electric strike, and door contacts.

New capabilities of traditional devices, and the introduction of completely new types of system components, are markedly improving restroom access for people with disabilities. Although the control of automatic doors in restrooms has traditionally employed much all of the same components as those used in entrance/egress applications, current restroom control systems leverage a range of components that have been designed to serve these specific requirements.

A system includes 4 basic components:

- An electrified lock - this can be a strike, magnetic lock, or electrified cylindrical or mortise lockset
- An activation device to energize the electrified lock - this can be a push button, push plate switch, or presence detector, such as a PIR or ultrasonic detector
- A visual 'occupied' or 'vacant' indicator – which can be a LED annunciator outside the locker room to let building occupants know that the room is unavailable.
- A visual 'locked' indicator -- This indicator is placed inside the room to let occupants know that the door is locked.

Secured or Unsecured Locks Systems

- Unsecured (unlocked) rooms entered by a manual lockset or electronic activation device -- By far, the most common
- Secured (locked) rooms entered by using a keypad, card reader or remote activation device (wired or wireless). Often used to control vagrancy and other unauthorized use of the room

Wireless Systems

Sometimes it can be difficult to run wired systems. Advances in wireless technologies have enabled the introduction of normally unlocked, restroom control systems with battery-powered wireless activation switches. 'Occupied' / 'vacant' annunciation outside the restroom, and 'locked'/ 'unlocked' annunciation inside the restroom can be provided by door jamb mounted narrow 1/2" LED annunciators, making wireless installations possible and compliant.

Applications and Opportunities

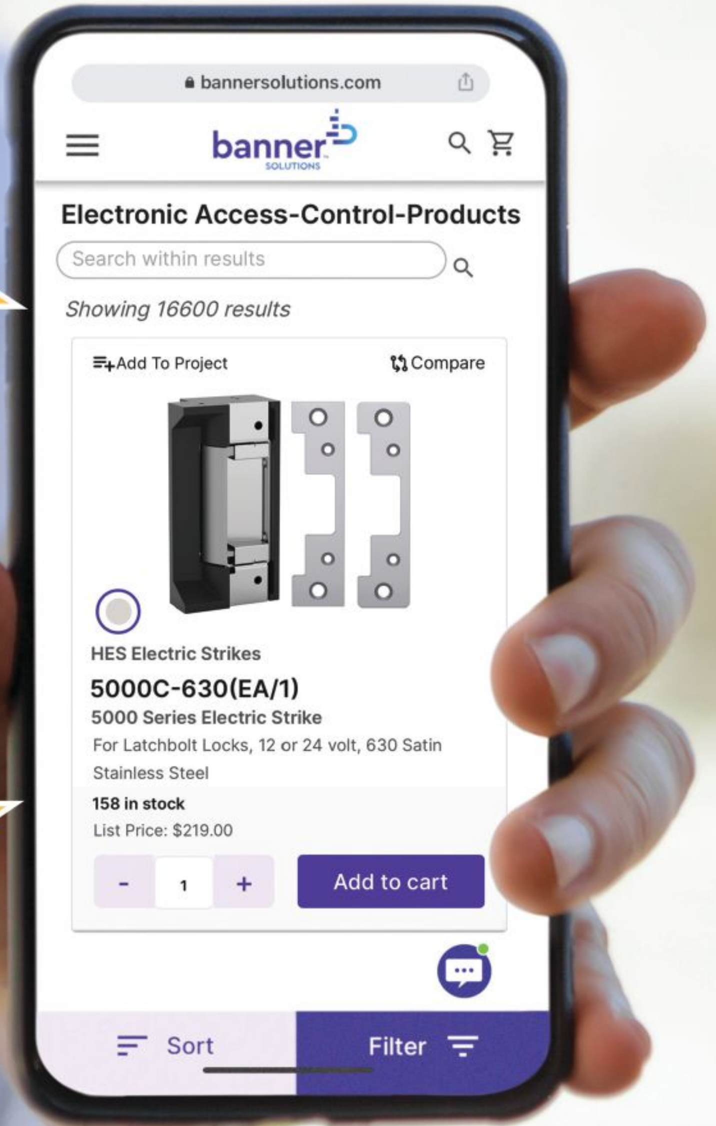
There's a wide range of applications for restroom control privacy systems. These include shared restrooms (2 doors accessing a common restroom), nursing stations, and ADA-compliant 'Universal' restrooms (barrier-free systems with automatic door operators) that are common in healthcare facilities mandated by building codes in commercial buildings. Other configurations for remote door locking include interrogation rooms, dressing rooms and meeting rooms.

As building codes and requirements continue to evolve, it's critically important for facility teams and systems integrators to stay abreast of the latest solutions to ensure that restroom control/privacy systems are delivering what's needed for users as well as for compliance. ***AC***

WORKFLOW SIMPLIFIED

NEW **BANNERSOLUTIONS.COM**

View the results of items available from over **260** brands.



Electronic Access-Control-Products

Search within results

Showing 16600 results

HES Electric Strikes

5000C-630(EA/1)

5000 Series Electric Strike

For Latchbolt Locks, 12 or 24 volt, 630 Satin Stainless Steel

158 in stock

List Price: $219.00

View the number of items in stock and ready to **ship today!**

Scan to learn more

YOUR PRODUCTIVITY PARTNER

Explore our expanded website features designed to help you find the products you need across our industry leading inventory selection.

banner™ SOLUTIONS

h.e.s. ASSA ABLOY

Request information: www.securityinfowatch.com/12071932

Industry Insights: ACRE President, Americas, John Skowronski

With so much change, ACRE is at a pivotal moment in the company's history as the new President explains in this exclusive interview

by Paul Ragusa

There have been some major changes these past few years at ACRE, parent company to well-known brands including RS2 Technologies, Open Options, ComNet, Razberi and Feenics. About a year ago, ACRE founder and longtime CEO – and voice and face of the company since its formation in 2012 – Joe Grillo announced his retirement. Grillo, who helped lead the organization's growth to more than 500 employees in more than 25 countries, passed the reins over to new CEO Don Joos, who has held leadership positions at TPx Communications and PGi, both Siris portfolio companies, as well as at ShoreTel and Avaya. As ACRE's Chairman of the Board of Directors, Tzachi Wiesenfeld, pointed out at the time, "Don joins the company at a pivotal time and is primed to deliver great leadership capacity."

Grillo's retirement followed on the heels of ACRE getting acquired by UK-based private equity firm Triton, which has approximately 50 companies in its portfolio with combined sales of more than €18 billion, with more than 100,000 employees. Since the Triton deal, ACRE has made several notable acquisitions, including bringing on cloud pioneer, Feenics, for example, further solidifying its foothold in the access control market.

In April, ACRE announced a new President, Americas, John Skowronski, a respected business executive and technology leader with more than 30 years of experience in senior leadership roles. He most recently served as President of Stanley Security North America, where he oversaw the company's operations for the US, Canada, and Mexico. Over the course of his career, he has held senior-level roles with ADT, Tyco International, UTC and Stanley Black & Decker. In addition to Skowronski, ACRE added a Chief Technology Officer, Darren Learmonth, an experienced technology leader with a demonstrated history of product development and innovation within the security and the Internet of Things segments, previously holding executive roles with Nortek, HID, ASSA ABLOY and Silicon Labs.

Security Business magazine caught up with Skowronski to pick his brain on the future of one of the largest global access control companies in security, as well as his thoughts on how ACRE has been able to steer the ship through all these changes the past few years.

ACRE announced a new President, Americas, John Skowronski.

Security Business: ACRE has added several key executive positions since April, particularly with you and Darren Learmonth as CTO. Does this represent a shift in the company's strategy moving forward?

Skowronski: This year, our focus lies on establishing essential foundations for our business and that includes investing in individuals who possess expertise in this field or related industries. Striking a balance is crucial. We recognize the importance of having a team well-versed

/ProAccess SPACE
SALTO
Users
Audit trail
Read key
Delete key
Zones
SALTO XSperience Centre
Valid Until
Aug 07
1 2 3
4 5 6
7 8 9
* 0 #
SALTO inspiredaccess

in the ins and outs of the security industry while welcoming those from outside the market who can question our existing approaches and norms.

The ACRE security team was built to help us view things from diverse perspectives. We have the advantage of fresh eyes that bring unique insights. This foundation enables us to tackle problems more effectively, as people are encouraged to challenge the status quo.

SB: Many companies in this industry (like ASSA ABLOY and Johnson Controls, etc.) are a roll-up of several brands, and each brand has its own identity within the company. What is your vision for the future of ACRE and its many different brands?

> “We possess a clear vision of our position in terms of cloud access control versus on-premises access control.”
> — John Skowronski

Skowronski: People have perceived ACRE security as primarily being a holding company. However, the fact is that ACRE is a fully operational global business. We offer a diverse range of portfolios that address critical verticals and essential business challenges for our customers. We possess a clear vision of our position in terms of cloud access control versus on-premises access control. And we have distinct strategies for market segments, visitor management, and intrusion. These areas represent the core aspects of our business.

At ISC West this year, we unveiled our refreshed brand and a mission to unify our product brands under the ACRE umbrella to create fluid solutions that are agile and responsive to the industry’s evolving needs. We’re still committed to providing the highest level of security for customers, helping them eliminate customer risk with our expertise and experience. We still deliver a single, powerful solution set that aims to help customers protect what is most important to them – their people and assets.

SB: Likewise, ACRE seemed to be a collection of predominantly access control brands – many of which (Vanderbilt, Open Options and others) had overlapping technologies and capabilities. What is the vision or roadmap for the access control technologies at ACRE?

Skowronski: Looking back at the company’s history, it was originally established with a competitive mindset. However, as we strive for long-term, scalable growth, we need to cultivate a focused approach.

Our customer base is broad and where they are in their digital transformation efforts varies. Some of our customers still rely on on-premises systems while others are pure cloud. Therefore, our objective is to provide our customers with clear migration paths toward more advanced solutions, particularly in the realm of cloud technology. With ACRE, you have access to a single portfolio of intuitive on-premises, cloud, and hybrid security solutions. So, you have everything you need to keep your most important assets safe.

SB: How does technology like Comnet and Razberi fit into that mix?

Skowronski: Comnet and Razberi play a significant role in the mix. Comnet offers valuable networking and connectivity solutions that enhance the overall functionality and performance of our systems. Razberi offers complimentary technology to ComNet’s and its cybersecurity protection software, system health monitoring, and servers enhance the value of our brands. Both products allow us to optimize our operations, enhance customer experiences, and facilitate the migration toward more advanced and future-proof solutions.

SB: What lessons from Stanley, Tyco, ADT, etc., will help you in this new role at ACRE?

Skowronski: Throughout my career, I have been fortunate to collaborate with numerous leading organizations. Many of these businesses have undergone the process of consolidating multiple brands and businesses into a unified entity. Drawing from my past experiences and active involvement in driving such initiatives, I am well-equipped to support acre security in its consolidation endeavors.

I’ve also been through industry changes before. As the physical security industry moves toward a software-centric approach, relying less on hardware solutions alone, I can help ACRE in navigating this evolving landscape. It is crucial that we understand the changing needs and preferences of our customers and dealers as the industry undergoes these shifts.

SB: Do you foresee the same level of M&A activity moving forward for the company, and are there certain technologies or vertical market areas where you are looking to grow or expand?

Skowronski: We are actively focused on both organic and inorganic growth, with an active pipeline of opportunities in North America and Europe. We will continue to pursue M&A deals and remain engaged in the market as we progress through the next three years. Our approach is driven by recognizing the fragmented nature of the industry and evaluating opportunities for consolidation. Additionally, we are keen on leveraging innovative technologies that can expedite our time to market by seamlessly integrating with our solutions. We are also interested in technologies that can help expand our addressable market. These areas remain a constant source of interest for us. **AC**

BATTLE-TESTED
SECURITY
Welcome!
EZ™ HELP
LETTERS
NAMES
CALL / HANG-UP
VOLUME
TTY
VIKING
MODEL C-2000B
ADVANCED DOOR/GATE AND ENTRY PHONE CONTROLLER
VIKING
MODEL C-1000B
Call
Call

NEW!

Get Every Access Control Solution From the Name You Know…

NAPCO ACCESS PRO

Mobile | Cellular | Cloud | Wireless Locking | Embedded | Enterprise

Top-Rated Wireless Online Locking

Embedded, Web-Browser-Based Access Systems

Continental Enterprise Integrated Access/ Security/Video Platform

- Scalable, Access Control & Security Solutions from a Few Doors to Thousands
- Range of Options: Continental Enterprise with Web Client, Web-Browser-Based, Self-Contained Systems, Cloud-Based Hosted Systems (ACaaS)
- Integrated Video, Security & Wireless Locking
- Universal Identity & Visitor Management
- Choice Of Synergistic Panels & Platforms
- Super-Fast Processing - Key In Peak High-Demand Periods
- High Security Options; Mifare & DESfire Support
- Global Lockdown & Threat Level Management
- Robust Multi-Database Partitioning – For Different Offices or Departments, etc.
- *Numerous Technology & Integration Partners for Easy System Upgrades & Retrofits*

NAP DEALER
NAPCO ACCESS PRO

Get Started **Integrators Join Our All-New Dealer Program**

call 1.800.645.9445 | www.napcoaccesspro.com

NAPCO
SECURITY TECHNOLOGIES

Request information: www.securityinfowatch.com/10213301