

ACCESS CONTROL

TRENDS & TECHNOLOGY

2025

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

- Reframing Access Control: Enabling Intelligent Access and Exceptional User Experiences **P. S10**

Access Control Beyond The Door

*The future technology is mostly cloud-based,
with a dose of intelligence*

- The Cloud-Native Revolution: Transforming Physical Security and Enterprise Risk Management **P. S14**
- The Real Change That Cloud-Native Access Control Platforms Are Bringing **P. S20**

www.LocksmithLedger.com | www.SecurityInfoWatch.com

July/August 2025

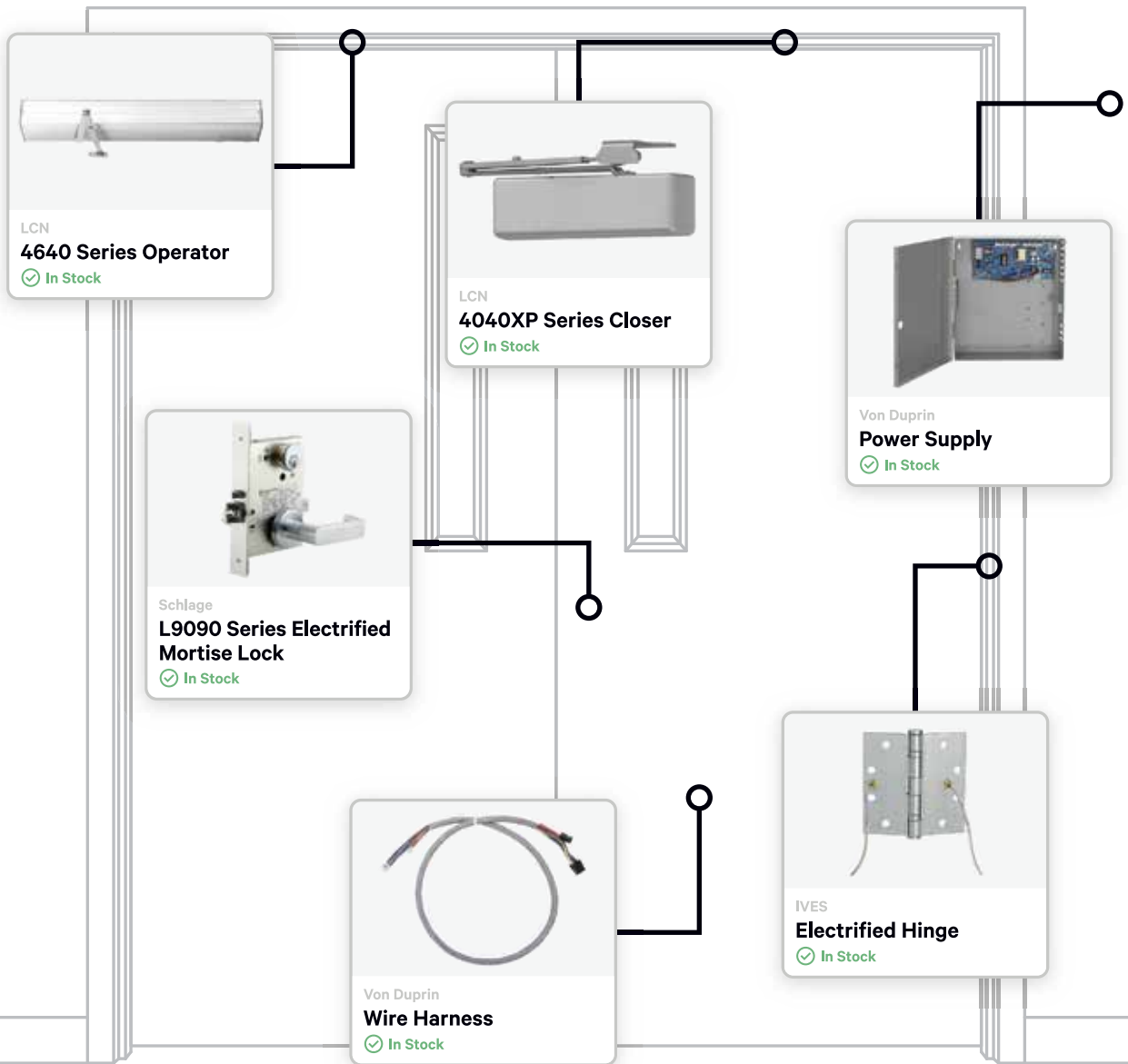
 ENDEAVOR
BUSINESS MEDIA



**Curb to
Cloud:**
Lock Up Business & RMR

 **NAPCO**
Access

Alarm Lock
Continental Enterprise
Marks USA



THE Source for Access Control and Security Hardware.

SECLOCK is the destination for all door hardware. Discover an extensive in-stock inventory from all leading manufacturers, work with our team of technical experts, and experience same-day shipping for any item you need.

SECLOCK is THE logical choice.



LCN[®]

VON DUPRIN[®]

THE INDUSTRY'S FIRST 1/2" SURFACE MOUNT RIM STRIKE WITH PRELOAD



INTRODUCING THE REMARKABLE 1299 SERIES



CX-EPD1299L



CX-EPD1299L-BK

Camden Door Controls has launched a 1/2" version of our award-winning surface mount RIM strike with preload. The **1299 Series** Grade 1 strike offers 'Universal' design that delivers superior performance under the most demanding conditions

The patented design of **1299 Series** RIM strikes will release with up to 15 lbs of preload pressure, caused by differences in air pressure, inexact installation, or misaligned doors (during or after installation).

- » UL 1034 & 294 Security Listings; ANSI/BHMA A156.31
- » 12/24V, AC/DC, Fail Safe/Fail Secure
- » Latch monitor included
- » 1/4" and 1/8" spacer plates included, to accommodate up to 3/4" Latch Projection
- » Metal Marking Jig Included
- » Exclusive 5-Year, No-Hassle Product Warranty

Visit us online at www.camdencontrols.com



Scan this QR code for more information, including spec sheets, manuals, cross reference guides, and more!

LOCKING | CONTROL | ACTIVATION | ACCESS





ACCESS CONTROL 2025

TRENDS & TECHNOLOGY

Access Control Beyond The Door

ACCESS CONTROL

8 Intelligent Data, Intelligent Buildings: How Access Control Systems Can Improve Modern Workspaces

PAAV GANDHI

10 Reframing Access Control: Enabling Intelligent Access and Exceptional User Experiences

LEE ODESS

14 The Cloud-Native Revolution: Transforming Physical Security and Enterprise Risk Management

GEVA BARASH

20 The Real Change That Cloud-Native Access Control Platforms Are Bringing

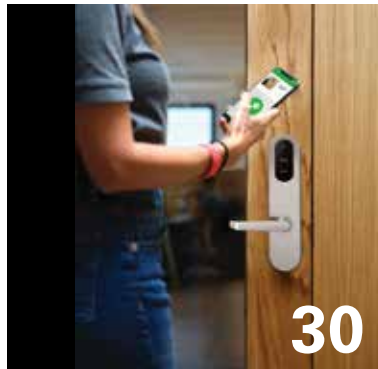
SETH RISER

24 How AI Has Transformed Traditional Access Control Security Implementations

BLAINE FREDERICK

30 Smart Locks Come of Age

PAUL RAGUSA



COLUMNS

6 My Point of View Head (End) in the Clouds
STEVE LASKY

DEPARTMENTS

6 Advertisers' Index

36 Product Showcase

COVER PHOTO: Gettyimages-1279139233

ACCESS CONTROL 2025

TRENDS & TECHNOLOGY

PUBLISHED BY



30 Burton Hills Blvd, Ste 185
Nashville, TN 37215
800-547-7377

Access Control – Trends & Technology 2025 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

Rodney Bosch

SALES

Group Publisher

Jolene Gulley-Bolton

(480) 524-1119

jgulley@endeavorb2b.com

Eastern US & East Canada

SB, STE, SecurityInfoWatch

Sarah Flanagan

(207) 319-6967

sflanagan@endeavorb2b.com

Western US & Western Canada

SB, STE, SecurityInfoWatch

Kevin Freel

(920) 212-2241

kfreel@endeavorb2b.com

Locksmith Ledger

Sales Manager

Travis Gipson

(318) 840.3158

tgipson@endeavorb2b.com

PRODUCTION

Production Manager Jane Pothlanski

Ad Service Manager Deanna O'Byrne

Audience Development Manager Delicia Poole

Art Director Marianne McIntyre

ENDEAVOR BUSINESS MEDIA, LLC

CEO Chris Ferrell

COO Patrick Rains

CRO Paul Andrews

Chief Digital Office Jacquie Niemiec

Chief Administrative and Legal Officer

Tracy Kane

EVP Design & Engineering and Buildings,

Lighting & Digital Infrastructure Group

Tracy Smith

Subscription Customer Service

Toll-Free 877-382-9187; Local 847-559-7598

Circ.SecDealer@omeda.com

Endeavor Reprint Services

reprints@endeavorb2b.com

Turn Every Door into Recurring Revenue with Napco's 2 MVP Cloud Platforms



Works with NAPCO's Full Line of Wireless Access Locks & Wired Access Panels — All at One Flat Per-Door Rate

Choose the MVP cloud platform that fits your job—and your business:

- **MVP EZ App** for smaller jobs made simple (no PC)
- **MVP Access** for enterprise-scale flexibility with video (no onsite server or database)

Both deliver fast installs, **convenient remote management**, & **profitable RMR services** that keep customers happier—and for the long run.

And because MVP's **cloud-based software is always up to date** and engineered under the same roof as Napco's locks and access panels, it **integrates seamlessly** and works natively with the hardware—right out of the box.

Go Live in 4 Easy Steps for RMR

1. **Sign in &/or sign up for Napco Cloud services*** and select the number of doors needed
2. **Install a wireless or wired Lock Gateway** central to the protected openings (one controls many)
3. **Choose wireless, keyless Trilogy Networkx locks with Built-in HID Prox Readers or Marks Deadbolt** and easily replace standard door hardware (&/or choose readers & access panels)
4. **Enroll devices & users in MVP software** — even from your phone

Scale up anytime for more doors, users; add schedules, SMS alerts & lockdowns.



Quote & Win More Access Jobs & RMR Easily:
Scan the QR Code or Call 1.800.645.9445



Alarm Lock | Marks | Continental

Get Started!

Trilogy, MVP Access & MVP EZ are trademarks of NAPCO. *Cloud Services require one-time sign up on www.napcocomnet.com



Beyond the Door: The Evolution of Access Control in the Cloud Age

BY STEVE LASKY



For decades, physical access control was a relatively static domain. A lock and key gave way to magnetic stripes and proximity cards, but the essential function remained unchanged: to grant or deny entry based on a binary credential check. Today, however, the world of access control has undergone a seismic transformation, evolving into a data-rich, cloud-native platform that extends far beyond the door.

This shift didn't happen overnight. The digitization of the workplace, the rise of hybrid work models, and growing concerns about the convergence of physical and cybersecurity threats have all driven the need for smarter, more agile access solutions. Traditional on-premises systems, with their high maintenance costs and limited scalability, couldn't keep up. Migration to the cloud provided a flexible and scalable foundation, and with it came the integration of artificial intelligence and real-time data analytics.

Modern access control platforms are now part of broader enterprise security ecosystems. They utilize AI to identify anomalies, automate responses, and anticipate potential threats. For example, if an employee badges into a building in Chicago but logs into a workstation in New York minutes later, AI can flag this as suspicious. Similarly, machine learning

algorithms can identify unusual patterns in access behavior, such as after-hours entries or multiple failed attempts, allowing security teams to intervene proactively.

Cloud-native platforms also offer remote management capabilities, faster software updates, and integrations with identity management and video surveillance systems. This has proven invaluable for global organizations managing diverse facilities and distributed workforces.

Looking ahead, access control will become even more frictionless and intelligent. Biometric authentication, already gaining traction, will grow more sophisticated and privacy-centric. Mobile credentials will overtake physical badges, offering encrypted, location-aware, and revocable access on smartphones. Data analytics will evolve from retrospective analysis to predictive modeling, enabling real-time risk-based access decisions.

Ultimately, access control is no longer just about "who gets through the door"—it's about using data to understand better and secure the flow of people, assets, and information. As AI continues to mature and cybersecurity becomes inseparable from physical security, the access control platform of the future will be less about hardware and more about insights. We've moved beyond the door—and there's no going back.

Advertisers' Index

Advertiser Name	Page
ACVS - Kantech	S33
Alarm Lock	S40
Altronix Corporation	S17, S19
Bulls-I Products	S37
Camden Door Controls	S3
DoorKing	S15
Marks USA	S7
NAPCO Security Technologies	S1, S5
Paxton Access	S13
Salto Systems	S23
SECLOCK	S2
STI, Safety Technology Int'l., Inc.	S25
Viking Electronics	S38
Wesco	S29

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



Smart Deadbolts for Growing Multifamily

Marks USA's new line of N-Series Deadbolt Locks is the opportunity locksmiths have been waiting for—built for the booming multifamily and multitenant markets—400,000 MDU units built in 2024 alone. Designed to help you secure every door more efficiently—and profitably—these smart solutions make it easy to work with architects, builders, and property managers.

- One-motion egress keeps you ADA code compliant
- Keyless access with standalone and interconnected models
- No key distribution costs or hassles
- No cylinder to pick—for greater security
- Less expensive door prep with deadbolt strength—saving time and labor (vs mortise)
- Proven, low-maintenance design with ANSI/BHMA hardware
- Exceptional battery life—up to 3 years on AA batteries with Power-Saver circuit
- Easy management with choice of 3 native Napco Access software platforms, enterprise, cloud, PC-free or App-only; for up to 5000 users & 7K time/date audit trail
- Flexible credential options—prox, fob, smart cards, or mobile access + Construction Mode

Keyless Interconnected & Smart Deadbolts



MARKS USA

www.marksusa.com | 1.800.645.9445

NAPCO
SECURITY TECHNOLOGIES

Marks USA a Division of NAPCO Security Technologies, Inc., Amityville NY USA





How Intelligent Building Strategies can



credit here

Create Secure Access Control Building Systems

Intelligent data is key for security professionals looking to prove the wider ROI and business benefits of an upgraded physical security system.

BY PAAV GANDHI

The Skinny

- Traditional access control systems only capture basic entry and exit data, offering limited insight into how spaces are actually used. Intelligent data goes further, tracking movement patterns and space utilization to provide a clearer picture of activity within a building.
- To get the most out of your data, you need to adopt a collaborative approach across departments. Continuous data collection and analysis helps reveal accurate usage patterns and better informs your decisions.
- Challenges to implementation include large upfront hardware costs, proving a system's ROI to decision-makers, and ongoing maintenance. However, advancements in automation and careful planning can mitigate these issues.

The user data available to security professionals is often limited to information about when people enter and exit the building, which

gives little insight into how a space is being used. This is because many access control systems only gather data at the first point of entry (the main building door) and private office doors. This baseline level of data only tells part of the story.

Why does data need to be intelligent?

Many access control systems will provide basic data on who enters and exits a building while helping to prevent security breaches. But forward-looking platforms will go beyond what happens at the door to provide granular insights into how a building is used. Intelligent data will tell you the route a person took and which areas are used most, when, and by whom.

What makes data intelligent?

For data to be 'intelligent,' it must be accurate, readily accessible, and easily digestible.

To be accurate, it should capture when a person was in a space with-

out the individual having to do anything themselves, such as badging a reader or signing in to a tablet. These are prone to human error, and people often forget to sign in or out. To ensure accuracy, data collection must be passive and in the background. For example, utilizing Bluetooth beacon-based location services alongside access control can provide valuable granular data about movement patterns.

To be readily accessible, it must be possible to extract and extrapolate without needing a specialist skillset.

To be easily digestible, it must be effortlessly understood by anyone, from front-of-house teams to stakeholders. This often means visual data such as breadcrumbs, heat-maps, and graphs.

How data is collected also comes into play. Intelligent data collection (i.e., automated collection) is far more efficient as it reduces the burden on front-of-house and admin teams, who might otherwise be manually monitoring space utilization, attendance, and facility use. It also makes life simpler for security teams who would otherwise spend a considerable amount of time cross-referencing video footage, time and attendance, access control, and Wi-Fi tracking data for post-incident analysis.

How can teams best maximize data?

Like with any project, it is best to have a clear outcome in mind from the outset. Without a clear goal, looking at reams of data can become overwhelming and ineffective. For security teams, this could be reducing the time taken to investigate an incident, with a clearer picture of where an individual went on a site. Or to gain new capabilities in auditing who used a space such as a secure area without imposing further security barriers such as an additional door and reader.

To further maximize the use of

data, security professionals can collaborate with wider teams to look beyond just security breaches.

For example, the goal could be to support facilities management in optimizing the office space to better suit the needs of its users. In this instance, data such as peak usage times and occupancy can be considered to build a picture of how the space is currently being used. The data might reveal an underused kitchen, which could be repurposed into a meeting room or more hot desk areas.

To keep data accurate, it is important not to rely on a single data point. Instead, teams should collect and analyze data frequently over time to understand patterns.

What are the challenges facing security professionals, and how can modern systems tackle these challenges?

The Challenge:

Pressure to prove ROI

As with any investment made by a business, proving return on investment (ROI) on security systems is an organizational demand. As traditional access control already serves a basic level of security, the reasons for investing in a new system are not always immediately obvious to decision makers. This leads to complacency and a belief that their security and user experience needs no improvement.

The Solution:

Benefits beyond just security

A physical security solution that not only enhances protection but also contributes to an organization's broader goals can deliver value beyond basic protection and present security professionals a more compelling opportunity to prove the potential ROI of a new system.

The Challenge:

A costly hardware bill

Large upfront hardware costs can

understandably be off-putting and make upgrading systems more challenging, especially if demonstrating ROI is a concern.

The Solution:

Subscription-based models

Some providers now offer a subscription-based model and no upfront hardware costs. This presents an opportunity to get up and running with next-generation physical security without having to explain an eye-watering hardware bill to stakeholders.

The Challenge:

Ongoing maintenance

Ongoing maintenance on security systems has also historically been a challenge. Traditional on-premise security systems require manual updates and patches, which are labor- and time-intensive. These systems can also be unsecure, as they are not automatically updated and can fall behind in terms of patches and upgrades.

The Solution:

AUTOMATE THE PROCESS

Cloud-based platforms reduce the burden of ongoing maintenance, with automatic platform and reader updates that can be managed remotely. It's a similar case when adding users to a new system and updating them.

Final thoughts

Intelligent data is key for security professionals looking to prove the wider ROI and business benefits of an upgraded physical security system. **AC**

About the author:



Paav Gandhi is Head of Product at end-to-end cloud access control platform Accessia.



Reframing Access Control: Enabling Intelligent Access & Exceptional User Experiences

Access control is no longer just about locking doors—it's about unlocking intelligence, identity, and enterprise value in a dynamic, hybrid world.

BY LEE ODESS



For the past 30 years, the electronic access control industry has been defined by one question: Can you get through the door? The answer was binary. A key, card, or fob, accepted or denied, determines your ability to enter a space. This logic was embedded in hardware, managed in silos, and built for a world where people worked from one building, Monday to Friday, 9 to 5, or vis-

ited spaces are already known and determined. We were an industry characterized by highly predictable patterns and a knowledge base that was left to do its job. And we did it well, by the way.

That world no longer exists on its own.

Let's focus on work for simplicity reasons, even though I can delve into any vertical and tell the same story.

Today's workplace is hybrid, fluid, and fast-changing. It is unpredictable. People aren't just employees, they're contractors, partners, vendors, and visitors. Even the employees are, to some extent, like visitors. Buildings aren't just offices, they're ecosystems of shared desks, hot zones, private suites, and remote nodes. Buildings are no longer isolated, either. They are part of a larger network with shared

Access control hasn't changed simply because technology has improved. It's changing because the world it serves has transformed.

Eonener

more complex, unpredictable, and rewarding. Some continue to play the incremental cottage game, which is understood but less relevant. No longer merely about keeping bad people out, locking and unlocking, access control has transformed into a platform for enabling intelligent access, data-driven insights, and exceptional user experiences.

It's time for a reframe. The door is still there, but it's no longer the center of the story.

From Locks to Legacy Logic

To understand where we're headed, we need to acknowledge where we've been.

Historically, access control was a hardware-based discipline. Proximity cards, turnstiles, badge printers, and metal keys dominated the scene. These systems were tightly bound to facility teams, designed to solve one problem: let the right person in, lock and unlock, and keep everyone else out, as they are considered bad.

Access was typically granted at the point of hire and changed only when an employee left or moved to a different department. Policies were rigid. Systems were often hosted on-premises and updated manually. Logs existed, but they weren't integrated, searchable, or context-aware. The idea of syncing access rights with HR systems, IT directories, or identity platforms was rare and difficult.

This "legacy logic" worked in an era of static work. Predictable work. But it wasn't built for today's reality: fast-changing roles, hybrid schedules, and high expectations for digital-first, frictionless experiences.

Why the World Has Moved On

Access control hasn't changed simply because technology has improved. It's changing because the world it serves has transformed. Four major forces are driving the shift:

1. Hybrid work & fluid space

A large number of employees, even those with back-to-work mandates, no longer work from the same building daily. Instead, they check into offices based on team needs, project sprints, or in-person events. This has created a new access reality: whoever needs access isn't always predictable, and permissions must reflect a dynamic work rhythm.

2. Blurring of physical and digital security

Threats are now multi-dimensional. Cyberattacks may involve physical access and vice versa. Tailgating, phishing-linked intrusions, and coordinated cyber-physical breaches are now real concerns. The traditional perimeter is no longer the building; it's the identity. IT convergence is not a trend; it's a reality.

3. Regulatory and compliance pressures

Frameworks like SOC 2, HIPAA, and GDPR demand clear audit trails: Who had access? When? Did they use it? Did they still need it? The days of siloed logs and unverifiable permissions are over. We may not like standards as an industry, but the external market does, and they are demanding them.

4. User expectations

Employees and visitors expect access to feel like every other tech interaction: seamless, mobile-first, integrated. No one wants to stand in line for a badge or download a plugin. Friction is no longer tolerated, and when it does appear, it reflects poorly on the brand and the workplace culture. We have never really known or cared about the end user. They were a card or a fob. They had no voice in how our systems functioned or worked. They do now, and it's due to mobile adoption. We are in the early innings of this influence, and it's not a small change.

amenities and services. Security threats are no longer just about physical breaches; they now span phishing, tailgating, identity theft, and insider risk. And critically, the systems we use to govern these spaces must evolve in kind.

And they have not.

In 2025, access control is at the forefront of an inevitable shift in paradigm. Some are playing mainstream games that are far



In short, the systems once designed for control must now support context, convenience, and connection.

The Reframe: Access As Intelligence

To keep up with these shifts, access control needs a new identity. It must move beyond locking doors and start enabling smarter, more informed decisions.

Here's what that transformation looks like:

Access begins with identity

In modern systems, access isn't tied to a badge; it's tied to a person. More specifically, their role, status, location, credentials, certifications, and context. When HR platforms, IT directories, and identity providers are integrated into the access stack, permissions can be adjusted dynamically. Someone who changes roles leaves a project or is de-provisioned from an application automatically has their access rights updated without requiring tickets or delays.

Identity-first access enables mobile credentials, biometric authentication, and Zero Trust principles to take root in the physical world. Something cybersecurity has long embraced. Again, this is inevitable.

Every door is a data point

Access is no longer just an event; it's a signal within the noise. When analyzed in aggregate and now moving to agentically with AI, access logs reveal trends:

- Which spaces are being used?
- Where is foot traffic creating risk or inefficiency?
- Are visitors being cleared appropriately?
- Is tailgating a problem in high-security areas?

This data supports more than just audits. It informs real estate decisions, security posture, and even employee experience design.

Today's workplace is hybrid, fluid, and fast-changing. It is unpredictable. People aren't just employees, they're contractors, partners, vendors, and visitors.

Access is part of the experience layer

The best access systems are nearly invisible. Always have been. They work so smoothly that users forget they're there. By integrating access control with workplace experience platforms, organizations can deliver:

- Touchless, app-based check-ins for guests or even seamlessly with biometrics.
- Personalized permissions based on calendar events or the purpose of the visit.
- Real-time notifications when someone arrives.
- Temporary access for service providers or deliveries.

Access becomes a seamless part of the user journey. Not a blocker but a facilitator. Our identity as one where bad experience is a form of security is over. The game is now about delivering security and convenience.

Unlocking Strategic Value Across the Enterprise

Reframing access control as a platform, not a point solution, opens the door to strategic value across the organization. This strategic value is permission for our industry to extract more value. If all we do is keep bad people out, lock and unlock, that value, that utility, has already been determined (roughly a \$10B opportunity). Still, if we move

to an exponential value around operational efficiency and revenue generation, all built on the utility of security, we can garner more value, upwards of \$100 billion.

Consider these examples:

Real estate and facilities

Access data can show which areas are used, when, and by whom. This insight supports thoughtful space planning. Access control can play a significant role in reducing footprints, repurposing underutilized areas, and enhancing collaborative spaces.

HR and people ops

New hires can be automatically granted access based on their role and location. Departures or transitions trigger instant revocation. DEI teams can evaluate access equity across the org: no more spreadsheets or manual handoffs.

IT and cybersecurity

With convergence accelerating, IT teams are demanding that physical access aligns with identity governance policies, SSO providers, and cybersecurity controls. Access rights can be tied to MFA status, training completion, or device posture.

Risk and compliance

Audit trails are no longer just "nice to have." They're expected, especially in regulated industries. Access control logs help prove compliance, identify anomalies, and support forensic investigations when needed.

Thinking Like a Platform, Not a Product

To deliver on this promise, the access control industry must think beyond door readers and badge types. What's needed is a platform mindset. This mindset embraces openness, modularity, and integration.

That means:

- APIs and SDKs that connect access control to IT, HR, visitor management, and analytics tools.

- Cloud-native infrastructure for easier updates, scaling, and remote management.
- Standards-based architectures that reduce vendor lock-in and increase interoperability.
- Composability, allowing organizations to build the proper access stack for their environment, rather than just accepting an off-the-shelf product.

The most innovative players, both buyers and builders, are adopting this mindset now. They're not asking, "Which badge reader should I buy?" They're asking, "What should access control enable in my organization?"

From Control to Capability

At its core, this shift represents a more profound truth: Access control is no longer just about limiting risk; it's about enabling value. It's about enabling safer workplaces, making

more intelligent decisions, achieving more agile operations, and delivering better experiences.

The question is no longer, "Can you get through the door?" It's "What happens after you do, and how do we ensure that moment is secure, seamless, and strategically aligned?"

That's the opportunity, and that's the reframing we need.

About the author:



Lee Odess is the voice of the global access control, transforming security through strategic vision and industry expertise. As CEO of The Access Control Collective (TACC), he leads brands that redefine how the access and smart lock industry evolves. His influence spans multiple channels including LinkedIn, the Access Control Executive Brief, weekly Security Breakdown newsletter, industry Slack community, ACS Events, and TACC's marketing division, Ready Shoot Aim. Known for challenging conventions while advocating for safer, seamless environments, Lee's vision is clear: "The next 30 years will have little to do with the last 30 years and there's no better time than now to be in the security industry." Learn more at tacc.me.

The Paxton Tech Tour

Your ticket to the security event of the year!



The highly acclaimed Paxton Tech Tour is coming to a location near you.

We'll show you a variety of security solutions your customers will love, including wired and wireless access control, video management and intercom.

- Free access control software (\$765 MSRP)
- Up to 80% off product
- Exclusive installer gift



Rated **4.9 out of 5** ★★★★★ by attendees

Get your free ticket today ▶

paxton-access.com/us/tech-tour





The Cloud-Native Revolution: Transforming Physical Security and Enterprise Risk Management



Gettyimages2180542869

BY GEVA BARASH

Why cloud-native access control is reshaping enterprise security for a hybrid, hyperconnected world.

In today's urban landscape, the traditional paradigms of physical security are undergoing a profound transformation. Organizations navigate an increasingly complex world marked by evolving threats, hybrid work models, and interconnected digital and physical infrastructures. The demand for more agile, resilient, and integrated security operations has never been more pressing. The forefront of this evolution is the emergence of cloud-native access control platforms, a pivotal innovation that is reshaping how we safeguard assets, manage personnel, and mitigate enterprise risk.

What Does “Cloud-Native” Truly Mean in Access Control?

In physical access control, “cloud-native” platforms are engineered from the ground up for cloud microservices, elastic scaling, and continuous delivery, whereas “cloud-hosted” offerings park legacy, on-premises software on a remote server without redesigning the core architecture. A true cloud-native access control platform is characterized by:

- **Microservices Architecture:**

Instead of a single, monolithic application, cloud-native systems are composed of small, independent, and loosely coupled services (microservices). Each service

handles a specific function (e.g., user authentication, door control, lighting, air conditioning, and event logging) and can be developed, deployed, and scaled independently. This modularity enhances agility, resilience, and maintainability.

- **API-First Design:** Cloud-native platforms are built with Application Programming Interfaces (APIs) as a core component, facilitating seamless integration with other enterprise systems (HR, visitor management, video surveillance, building management systems, identity providers). This open, interoperable approach breaks traditional security silos.
- **Industry Standards:** Another crucial aspect of the system is selecting



INTERNET OR CELLULAR SYSTEMS

DKS Telephone Access Systems can be connected with an internet or cellular connection. Both include the DKS Cloud that allows administrators to program the system from any internet connected device; laptop, tablet or smartphone! Team this with DKS' 900 MHz wireless access expansion to control access for up to 24 entry points.



PROXPLUS™ SECURE CARD READERS

For those applications that require a higher level of security than standard Proximity Card Readers and cards can offer. ProxPlus cards are programmed with a unique identifier, making them extremely secure and difficult to duplicate. And, since the DoorKing Card Reader outputs the card code in a 26-bit Wiegand format, they are compatible with almost any Access Control System on the market.



Telephone Entry

Gate Operators

Access Control

Traffic Control

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



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

TRAFFIC CONTROL

The DKS 1625 Wedge Barrier is designed to be used with the 1602-590 operator (sold separately). The Wedge Barrier is ideal in applications where a higher degree of vehicle traffic control is desired, but without the expense of bollards, wedges, or crash beams – making it ideal for apartment communities, gated condominiums, car rental agencies, parking lots, and toll booths.



DC OPERATORS

When it comes to securing a high traffic gate in any location, or with unreliable power, DKS manufactures a full-size DC Gate Operator. With the ability to switch from AC to DC seamlessly and pull a full-size gate for hundreds of cycles from backup batteries, DC also means the operator can be completely off the grid with a solar power supply.





non-proprietary products. By adding nonproprietary products, we guarantee that different services can be as easy as writing an API to adhere to the standard. Being able to add various services, such as light controls, timers and other products, through the API becomes an easy integration for the manufacturers.

- **Continuous Integration/Continuous Delivery (CI/CD):** Updates, new features, and security patches are delivered continuously and automatically through the cloud services, ensuring the system is always running the latest version with minimal downtime. This contrasts sharply with the infrequent, disruptive updates of on-premises systems.
- **Managed by Third-Party Providers:** The infrastructure, maintenance, and updates are typically handled by the cloud service provider, freeing organizations from the burden of managing physical servers, software installations, and complex IT infrastructure.
- **Elastic Scalability:** Resources can be automatically scaled up or down based on demand, eliminating the need for overprovisioning and allowing the system to handle fluctuating workloads efficiently.

Cloud-native access control isn't just about remote accessibility; it's about a dynamic, adaptive, and highly integrated system that truly leverages the cloud's inherent benefits for a more robust and responsive security posture.

The Business Case: Unlocking Strategic Advantages

The transition to cloud-native access control is driven by compelling business advantages that extend far beyond the server room:

1. Cost Efficiency and Predictability: By shifting from a capital expenditure (CapEx) model of purchasing and maintaining hardware/software to an operational expense

(OpEx) model, organizations can significantly reduce upfront and long-term costs. Cloud-native platforms typically operate on a subscription basis, offering predictable monthly costs that cover infrastructure, maintenance, and updates. This eliminates the need for expensive server refreshes, software licenses, and dedicated IT staff for system upkeep, leading to long-term operational savings.

2. Unprecedented Scalability and Flexibility: Cloud-native systems are inherently designed to scale. Whether an organization is expanding to new locations, experiencing rapid growth in personnel, or needs to manage access for a temporary event, the system can dynamically adjust resources. This flexibility extends to supporting hybrid work models, enabling seamless remote management of access policies across disparate locations.

3. Enhanced Operational Agility and Responsiveness: The microservices architecture and CI/CD pipelines inherent in cloud-native platforms enable rapid deployment of new features, policies, and security updates. This agility allows for security teams to respond almost instantly to emerging threats, adjust access privileges in real-time, and expedite incident response, thereby aligning security with business needs.

4. Reduced Vendor Lock-in and Increased Choice: Cloud-native applications, particularly those built with open APIs, foster greater interoperability and minimize reliance on a single vendor's proprietary ecosystem. This provides organizations with more flexibility to integrate best-of-breed solutions for video management, visitor management, HR, and other systems, creating a truly unified security environment.

5. Improved Business Continuity and Disaster Recovery: Cloud-native platforms are designed for resilience, often distributing workloads across multiple geographically

dispersed data centers and availability zones. In the event of a localized outage or disaster, the system can automatically fail over to a healthy instance, minimizing downtime and ensuring continuous operation of critical access control functions. This inherent redundancy far surpasses the disaster recovery capabilities of most on-premises systems.

6. Data-Driven Insights for Enterprise Risk Management: Cloud-native solutions facilitate the aggregation and analysis of vast amounts of access data. This data can provide invaluable insights into traffic patterns, anomalous behaviors, compliance gaps, and potential security vulnerabilities. Analytics tools, often powered by AI/ML within these platforms, can identify trends, predict risks, and inform proactive security strategies, transforming access control from a reactive tool into a proactive risk management asset.

Technical Superiority: Building a Resilient and Integrated Security Fabric

Beyond the business benefits, cloud-native access control platforms deliver significant technical advancements that enhance the overall security posture:

1. Robust Security Posture: Cloud providers invest heavily in cybersecurity, offering a level of infrastructure security that most individual organizations cannot match. Cloud-native designs often incorporate security into every layer of the application (DevSecOps), from secure API gateways that enforce authentication and authorization to continuous vulnerability scanning and real-time threat detection. Data is typically encrypted in transit and at rest, and features like multi-factor authentication (MFA) and Zero Trust Network Access are foundational.

2. Centralized Management and Decentralized Control: Security administrators can manage access policies, user credentials, and system configurations for multiple loca-



**WE'RE WITH YOU EVERY
STEP OF THE WAY**

As the industry leader in power and data transmission innovation, Altronix designs and manufactures electronic products that ensure security systems run at optimal performance. We pride ourselves on providing the best technical and customer support in the business. That's the Altronix advantage.

Run With It™



tions from a single, centralized cloud dashboard accessible from anywhere with an internet connection. Despite this centralized oversight, on-premises controllers ensure local decision-making and business continuity even if internet connectivity is temporarily lost.

3. Seamless Integration through

Open APIs: The API-first design ethos of cloud native platforms is a game-changer for integration. This allows for:

- **Unified Identity Management:** Seamlessly linking with HR systems for automated onboarding/offboarding, ensuring immediate access revocation when an employee leaves.
- **Enhanced Visitor Management:** Integrating with visitor systems to preauthorize guests, generate temporary credentials, and streamline check in/out processes.
- **Integrated Video Surveillance:** Connecting access events with video footage for rapid forensic analysis and real-time visual verification of alarms.
- **Building Management Systems (BMS) Integration:** Orchestrating environmental controls, lighting, and HVAC based on occupancy detected via access control events, optimizing energy use and operational efficiency.
- **Emergency Response Automation:** Triggering automated lockdowns, mass notifications, and emergency alerts based on specific access control events or breaches.

4. High Availability and Fault

Tolerance: Cloud-native architectures are built with redundancy in mind. If one microservice or component fails, others can take over, preventing system-wide outages. Load balancing distributes traffic, and automated failover mechanisms ensure continuous service delivery, contributing significantly to overall system resilience.

5. Simplified Maintenance

and Updates: With continuous

deployment, patches and feature enhancements are delivered seamlessly in the background, eliminating the need for manual updates or system downtime. This ensures the system is always protected against the latest threats and benefits from new functions without an administrative burden.

These deployments demonstrate how technical advancements drive tangible business outcomes.

The trajectory of cloud-native access control points towards even greater sophistication and integration.

Real-World Impact: Agile, Resilient, and Integrated Operations

Organizations are using cloud-native access control to modernize security and operations.:

- **Multi-Site Corporations:** A large retail chain can centrally manage access policies for hundreds of stores globally from a single interface, ensuring consistent security standards, rapid credential changes for new hires or terminations, and instant lockdown capabilities across all locations during an emergency, regardless of local IT support.
- **Educational Institutions:** A university can integrate its access control with student information systems, automatically granting or revoking dormitory access based on enrollment status, managing access to labs and restricted areas, and providing mobile credentials for students and faculty. During an active threat, the system can automatically initiate a campus-wide lockdown and notify authorities.

- **Commercial Real Estate:** Property managers overseeing multiple buildings can offer tenants flexible access solutions, integrate with tenant experience apps for seamless entry, and gain real-time insights into building occupancy and traffic flow. This enables more efficient space utilization, enhanced tenant services, and proactive maintenance scheduling, while ensuring robust security that meets the diverse needs of tenants.
- **Healthcare Facilities:** Hospitals can manage highly granular access to sensitive areas, track staff movement for compliance, and provide rapid and secure entry for emergency personnel. Cloud-native resilience ensures that critical access functions remain operational even during network disruptions, vital for patient care and safety.
- **Multi-Family Sites:** Multifamily management companies can manage apartment and site access, add or remove tenants through a central portal, and enable residents to control lights, temperature, and entry remotely via a mobile app.

The Future Outlook: Beyond Today's Capabilities

The trajectory of cloud-native access control points towards even greater sophistication and integration. We can anticipate:

- **Deeper AI/ML Integration:** Beyond current analytics, AI will drive more advanced predictive security, anomaly detection that identifies subtle deviations from normal behavior, and adaptive access policies that automatically adjust based on real-time risk assessment (e.g., environmental factors, threat intelligence feeds).
- **Identity-Centric Security:** Access control will increasingly converge with broader identity management solutions, forming a

comprehensive identity fabric that extends across physical and digital realms, enabling true Zero Trust architectures.

- **Hyper-Automation:** Workflows will increasingly connect access control with HVAC, elevator dispatch, and custom settings.
- **Enhanced Mobile and Biometric Integration:** Mobile credentials will become even more ubiquitous, leveraging smartphone biometrics and secure elements for highly convenient and secure access.
- **Sustainability Integration:** Cloud-native platforms, by optimizing resource usage and reducing on-premises hardware, will inherently contribute to more sustainable building operations, aligning with broader ESG (Environmental, Social, and Governance) goals.

Embracing the Agile Security Paradigm

The shift to cloud-native access control platforms is not merely a technological upgrade; it is a strategic imperative for organizations aiming to achieve truly agile, resilient, and integrated security operations. By embracing this approach, businesses can transcend the limitations of legacy systems, unlock substantial operational efficiencies, bolster their overall security posture, and gain actionable insights that drive proactive enterprise risk management.

As security professionals, our role is to guide organizations through this transformative journey, helping them leverage these powerful cloud-native capabilities to build smarter, safer, and more adaptive environments for the future. **AC**

About the author:



Geva Barash is the visionary Founder & CEO of Secure Our City, Inc., a leading security and technology services design firm dedicated to creating safer, smarter environments. With over two decades of experience at the nexus of Physical Security, intelligence, and cutting-edge technology, Geva is a recognized expert in designing integrated, proactive security solutions for educational, public safety, commercial, and government sectors. Geva is committed to advancing the industry by leveraging innovations, such as cloud-native platforms, to mitigate risk and enhance operational resilience

Altronix®

NETWAY SPECTRUM

Hardened PoE Switches
& Fiber Media Converters

- Deploy IP devices at remote locations with or without local power
- Supports up to 90W per port
- Rapid battery charging provides extended power backup
- 115/230VAC or 277VAC input
- Manage and reset devices remotely with LINQ™ Network Power Management
- Lifetime warranty

Run With It™

© 2025 Altronix Corporation – 983731-0725SB altronix.com



Why cloud-native access control is reshaping physical security in a post-pandemic, digital-first world — and why legacy systems can't keep up.

The Real Change That Cloud-Native Access Control Platforms Are Bringing

BY SETH RISER

What is “Cloud-Native”? How did COVID-19 reshape access control management? Why are legacy access control systems falling behind in today’s distributed world? Can physical security keep up with digital transformation? This article will break down what cloud-native access control really means, how it differs from legacy or cloud-hosted systems, and why it’s quickly becoming one of the most critical parts of modern security operations. The onset of the pandemic not only altered our work locations but also transformed the management practices of security personnel. Maria Lopez is the security director of an expanding healthcare network, and she has witnessed this directly. As her group swiftly established new clinics, she was compelled to reevaluate their approach to physical access. Her legacy access control system requires on-site servers, manual upgrades, and frequent

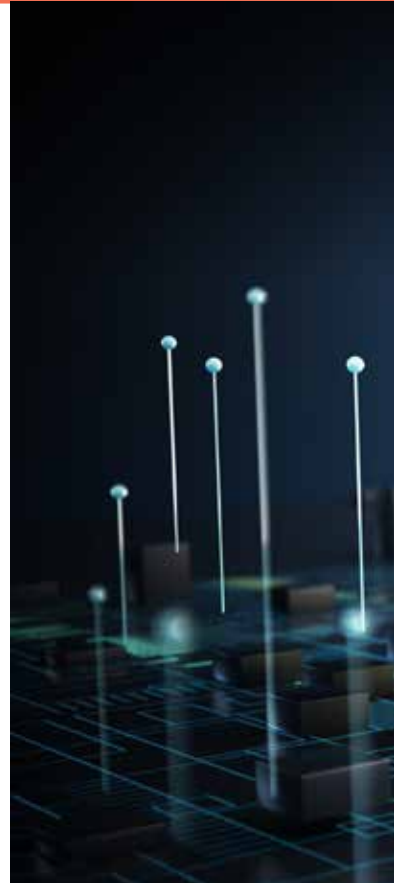
travel solely for credential changes. It became evident to her that this model could not maintain pace. She began seeking a more efficient method to rapidly scale access control, manage users remotely, and integrate security with standard business processes — a realization now acknowledged by many enterprises across all sectors.

Cloud-Native Specific

Cloud-native access control makes this possible. These systems are not simply cloud-hosted software. They are designed explicitly for cloud operation with more contemporary technology, which allows them to expand, integrate, and adapt far more rapidly than their legacy (on-prem) or cloud-hosted equivalents. Conventional systems may transition to cloud servers, but that doesn’t change the fact that they continue to depend on cumbersome, monolithic software that requires manual updates and local

infrastructure. Cloud-native platforms utilize APIs, containers, and microservices to maintain agility and resilience. They are engineered for optimal uptime, automated updates, and seamless integration from the outset. If you’re unfamiliar with containerization and microservices, it’s worth its read; it is, quite simply, the future.

“We are transitioning from systems tailored for security specialists to intuitive platforms manageable by IT professionals,” says Sean Peterson, Director of Product, Marketing, and Support at Aiphone. Cloud-native systems eliminate the need to install servers at each location. For Maria, this meant she could establish access control for new facilities within days rather than weeks. New locations can be preconfigured and activated remotely, conserving time and circumventing logistical challenges. However, it’s more about team adaptability, rather than launching a new site





Cloud-native platforms utilize APIs, containers, and microservices to maintain agility and resilience. They are engineered for optimal uptime, automated updates, and seamless integration from the outset.

adventr

quickly. Cloud-native solutions enable businesses to scale without requiring changes to hardware or IT architecture. Imagine being given a five-site expansion to manage right now... No problem at all. Merging into fewer offices? Just change permissions and access points through the dashboard.

Centralized management is just as important here. Maria and her staff can now oversee and regulate access across numerous clinics from a centralized dashboard, enabling real-time modifications without departing from the office. This "single pane of glass" enables security personnel to give or revoke access, respond to alerts, and evaluate trends from a unified interface. A previous client of mine, a retail corporation that transitioned to a unified cloud-based platform, saw a reduction of approximately 50% in its daily security management workload by changing its workflows and adopting a converged and uni-

fied approach. This is extremely valuable in sectors where staff turnover is common. Universities have thousands of users to manage each semester, and these Cloud-native systems allow the effortless onboarding and termination of access in synchronization with enrollment workflows.

Maintenance Made Easy

There is a significant difference in how these systems handle maintenance. Legacy systems require scheduled upgrades, IT coordination, and system interruptions. Cloud-native infrastructure has automatic updates. It's always current, always secure, and always available. Security teams utilizing cloud-native solutions often employ a continuous delivery strategy, which eliminates the need to wait for quarterly software rollouts or manually address vulnerabilities. New features are integrated effortlessly, and essential security

updates are automatically implemented throughout the entire system. For resource-limited teams, this results in more time devoted to strategy and less time on managing obsolete infrastructure. These solutions can even interface directly with HR systems, video management, analytics tools, and visitor applications. The system automatically activates an individual's access upon hiring. When they leave, it can immediately revoke their access, without any delays or errors.

A great example of this is a logistics company that can integrate access and video via the cloud, identifying anomalies in access and entry patterns associated with internal theft, allowing them to intervene much sooner than before. Assume a facility employs a human resources system, a visitor management platform, and a video surveillance network. A cloud-native access solution can integrate all of them. After onboarding a new employee,



access is granted according to their department and the schedule they are assigned to. If an employee attempts to enter a restricted area, the VMS will document and flag the occurrence, triggering an automated notification to their supervisor. This can occur autonomously, without human involvement; it's all about process management, but more importantly, having the time to do it, which can be achieved when you shift your workload away from the heavy load of managing an on-premises or hybrid system.

Data in the Clouds

The idea of storing key access data in the cloud makes some risk-averse teams nervous, and for specific niche industries in critical infrastructure, it is impossible. A true cloud-native platform has E2EE (end-to-end encryption), MFA (multi-factor authentication), and RBP (role-based permissions), as well as certifications used by banking and IT systems in the healthcare sector. Suppose the provider meets standards such as SOC 2 or ISO 27001 and agrees to sign data processing agreements. In that case, cloud-based solutions can offer stronger security than the patchwork of local server systems used by most businesses today. The next big concern is internet disruptions. However, cloud-native services generally provide offline modes that enable local hardware to persist in allowing or denying access based on cached credentials. Once the connection is back up, all data synchronizes and updates automatically. Most solutions also provide cellular failover or hybrid alternatives just in case you have a location with unreliable connections. One of the biggest misconceptions about cloud-native systems is that not all card readers or controllers will be compatible. Of course, organizations must assess their infrastructure and identify reusable components. The reality is that many

cloud-native platforms accept standard protocols and hardware such as Mercury or OSDP. Retrofitting is usually very feasible, and incremental upgrades allow you to transition progressively rather than all at once. Now, here's a significant caveat: the subscription pricing model necessitates a shift in mentality from what most end-users are accustomed to. Organizations pay a monthly cost based on the number of doors or users, rather than purchasing hardware and licenses upfront. This transitions security from a capital expenditure to an operating expenditure. While some in the industry dislike the idea of recurring monthly expenses, others believe that the elimination of server maintenance, travel time, and system downtime significantly compensates.

Open It Up!

That brings us to the last red flag, so to speak, vendor lock-in. While most of the industry has moved away from this in favor of open integration and API-enabled frameworks, some manufacturers still restrict your ability to export data or interface with external systems. It is essential to prioritize suppliers that endorse open APIs and maintain transparent data ownership policies. Selecting a platform with an open architecture ensures flexibility and longevity, eliminat-

ing the need for ongoing support from a hardware manufacturer for discontinued devices. So, what lies ahead? These days that's harder than ever to predict but, based on my experience and current clients I can confidently say the following: mobile credentials are supplanting plastic badges, AI-driven analytics are being implemented to identify irregularities such as tailgating or after-hours access and cybersecurity systems are increasingly integrating with access control to enable zero trust models, which maintain both physical and digital identities simultaneously. Teams gain more visibility, power, and time to focus on strategy instead of troubleshooting outdated systems. The shift is occurring across various industries, including healthcare, logistics, education, retail, and others. Organizations are realizing that cloud-native systems help them respond faster, scale smarter, and adapt to whatever comes next. As Steve Van Till, the Founder and CEO of Brivo, put it, "Organizations need the ability to manage security and access control remotely... this is accomplished through the cloud." For security professionals contemplating their next move, the answer is straightforward. If your current system can't keep up, cloud-native access control might be the direction change you've been looking for. **AC**

About the author:



Seth Riser is an accomplished professional with extensive experience in strategic development and operations within the security sector. Currently serving as a Principal Consultant at Why Strategy Matters, Riser empowers small to medium-sized businesses (SMBs) and mid-market organizations through actionable business strategies. As Vice President of Operations at ESI Convergent, Riser drives operational growth at the intersection of security manufacturing and consulting.

As the Senior Director at ARMSTAR, Riser leads the strategic direction for software and hardware development in the private security sector. Riser's previous positions include Vice President of Operations and Research and Development at Stratigos Dynamics, where oversight involved optimizing guard services and pioneering security solutions. Additionally, Riser has provided expert consultancy for the oil and gas sector, served as a Sergeant at the Texas Department of Criminal Justice, and held a Lieutenant position in the Louisiana Department of Public Safety and Corrections, overseeing high-risk inmate management.

SALTO **W**ECOSYSTEM



Smart building management solutions

Salto delivers the most advanced, flexible, and secure access control solutions for all types of industry applications.

salto 
INSPIRED ACCESS

salto.us



How AI Has Transformed Traditional Access Control Security Implementations



AdobeStock_1274732014

AI-powered access control is redefining safety, trust and performance in the workplace.

BY BLAINE FREDERICK

People need to feel safe. It's one of our most foundational and fundamental needs.

Before a company's compelling product, groundbreaking service, or disruptive technology makes a market impact, its people and spaces need to feel (and be) secure. It's always a priority, but companies struggle to address this issue in their messaging and practices.

According to the Harvard Business Review, 97% of employees say physical security is essential at work, while just 54% believe their employers share this opinion.

The result?

Employee productivity declines, turnover increases, and the brand's reputation suffers. Historically, companies have combated safety concerns with access control solutions. First, they protected their entrances with locks and keys,

rudimentary mechanisms that inevitably gave way to technology-driven solutions, such as keycards, PINs, and badge swipes.

Manual oversight often filled the gaps, with security personnel visually verifying identities or monitoring access points to ensure security. While these traditional methods provided a foundational layer of protection, their inherent limitations—such as lost cards, forgotten codes, the potential for human error, and their reactive nature—are becoming increasingly apparent.

A Paradigm Shift in Access Control

Artificial intelligence (AI) is now transforming access control and physical security. This isn't a subtle change or an incremental improvement.

In 2025, AI is doing more than augmenting access control and



Rely on STI®



...to help secure
access control points

G3 Multipurpose Push Button Helps Secure Doors

The G3 multipurpose push button is offered with three reconfigurable operation choices (Key-to-Reset, Momentary or Turn-to-Reset). Available with six shell colors, standard or custom label, and protective covers (with or without sound) to help prevent misuse and accidental activation.

- Key-to-Reset, Momentary or Turn-to-Reset
- Flexible mounting (flush or surface)
- Cover options with or without sound
- Constructed of polycarbonate material
- Choice of standard or custom label
- UL/cUL Listed, ADA Compliant



Safety Technology
International

Learn more at sti-global.com
or call 248-673-9898



physical security. It's reimagining what's possible, allowing next-generation access control systems to move beyond simple authentication and offer intelligent, context-aware security that supports broader operational goals.

The Evolution from Traditional to AI-Powered Access Control

For thousands of years, people have prioritized access control. The Egyptians leveraged sliding stones and a wooden pin lock to secure their doors. Robert Barron introduced lever tumbler locks, which required a key to lift internal levers to a precise height in 1778, and Linus Yale patented a cylindrical pin tumbler lock in 1848.

Access control was electrified in 1952 when Frank Best introduced the first electronic access control system, which allowed keyless entry and alarm integration. In other words, humans have been inventing and refining access control solutions for a while. Of course, today's access control technologies are significantly more sophisticated than a stone.

Modern access control began to shift in the late 20th century with the introduction of magnetic stripe cards, keypads, and RFID readers. However, these systems still relied heavily on physical credentials and were limited in gathering and analyzing real-time data, as well as in dynamically adjusting access rights.

While groundbreaking when they first emerged, traditional access control systems often struggle to keep pace with the sophisticated security challenges faced by modern organizations. Today, issues such as tailgating, credential sharing, and the inability to quickly adapt to new threats highlight their shortcomings.

Meanwhile, the need for the most sophisticated security solutions is more urgent than ever before. Incidents of workplace vio-



lence are on the rise, increasing by 11% between 2015 and 2019, with a subsequent spike following the COVID-19 lockdowns and work-from-home movement.

As a result, employee expectations, regulatory requirements, and the increasing sophistication of threats are making workplace security a non-negotiable priority. The latest technologies are making it more possible for companies to tackle all these problems simultaneously. AI-powered access control leverages facial authentication, machine learning, and behavior-based authentication to make real-time decisions and proactively identify and mitigate threats. These systems reduce human error and administrative burden, offering scalability and adaptability that traditional systems often lack.

More specifically, they allow organizations to become proactive in their security posture. Rather than reacting to threats after they occur, AI enables systems to learn, adapt, and make informed decisions in real time, fundamentally changing how organizations protect their assets, people, and premises.

In short, badges = "something you have," pin codes = "some-

thing you know," and biometrics = "something you are." Fundamentally, we are moving away from "something you have" and "something you know" to "something you are," which eliminates many shortfalls of legacy methods, such as items being lost, shared, stolen, or forgotten.

Key Transformations Driven by AI in Access Control

AI is in the midst of an undeniable hype cycle, making it easy to overpromise and underdeliver on the technology's potential.

Private investment is surging, reaching over \$130 billion globally in 2024, while AI investment from other entities, including public companies, corporate R&D, government funding, data center infrastructure, and talent development, is similarly surging.

This high spending creates an incentive structure that encourages overhyping the technology's capabilities, and the marketplace is flooded with products touting their AI capabilities. The result is a product and service ecosystem in which it can be challenging to differentiate real-world value from future promises and potential value.

AI's integration into access control is different. It's not a single innovation but a multifaceted evolution with real effects on how security is perceived and implemented. Some of the key transformations include:

Intelligent Decision-Making

AI can make decision-making more sophisticated by introducing a layer of data-driven discernment to access control.

For example, AI-powered access systems don't rely on credential checks, badge swipes, or code entries, which can be forged, stolen, or lost. Instead, AI-powered access control systems can dynamically assess the legitimacy of an access request by analyzing various data points, including:

- Contextual information such as the specific door or turnstile, the time of day, a user's GPS-verified proximity to the entry point, and the security level of the accessed area.
- Behavior patterns within the physical environment, such as an individual's typical entry and exit times for specific buildings or zones, common pathways taken through a facility, or even dwell time near sensitive access points, can be observed and learned.
- Environmental factors, such as localized security alerts for the area, unusual activity detected by nearby sensors, or extreme weather conditions that impact building access protocols, are also taken into consideration.

AI enables systems to assess user identity and access requests based on context, behavior patterns, and environmental factors, reducing false positives and enhancing security accuracy.

Enhanced Integration

AI-powered access control systems integrate seamlessly with video surveillance, intrusion detection, and building management plat-

forms to provide unified situational awareness.

This holistic integration provides unified situational awareness of the physical environment, offering security teams a comprehensive, real-time map-based view of access events, alarm statuses, and visual data. This leads to faster, more informed, and more effective interventions against physical threats.

Predictive Security

Machine learning algorithms identify anomalies and predict potential threats before they occur, enabling preemptive action.

Advanced AI models can go further, correlating multiple, seemingly minor physical anomalies to predict potential physical threats, such as an impending forced entry attempt or reconnaissance activity by a possible intruder.

Frictionless Access

Increasing security while introducing unnecessary friction into the process is a recipe for frustrated employees and cutting corners. AI-powered access controls accomplish both without compromise.

Facial recognition, biometric analysis, and tailgate detection enhance user convenience while maintaining robust authentication protocols.

Scalability and Adaptability

AI systems can evolve in response to changing organizational needs, user behavior, and evolving threat landscapes, offering long-term flexibility and resilience.

As new intrusion techniques or physical security risks emerge, AI models can be updated with new threat signatures or identify novel suspicious activities through anomaly detection capabilities.

This continuous learning ensures the physical access control system remains effective over time, protecting the organization's premises, assets, and personnel against current and future physical risks without requiring frequent, costly system overhauls.

Navigating Ethical Concerns with Care

As AI systems become increasingly powerful and mainstream in security applications, there is a corresponding increased focus on their ethics. Put differently, employees want security but don't want to compromise their privacy, and regulators are increasingly scrutinizing the deployment and governance of AI technologies.

Parsing the ethics of a constantly changing technology can be difficult. They encompass everything from how the data used to train AI models is collected and whether it's representative of all demographics and use cases to the types of decisions the AI models are authorized to make and specific considerations around technologies like Generative AI. For companies looking to leverage the AI-powered access control technologies to make their facilities safer, key ethical considerations include:

Data Privacy and Collection

Data privacy regulations, such as the European Union's General Data Protection Regulation (GDPR) and California's Consumer Privacy Act (CCPA), impose strict rules on data privacy and collection, particularly concerning AI-powered access control systems and biometric data.

Companies must ensure that biometric data is collected lawfully, stored securely, and processed with explicit consent from the user.

Employees, visitors, and other stakeholders have the right to access, rectify, erase, and restrict the processing of their data. Additionally, companies must inform users about their data usage and provide clear, transparent privacy policies.

Before implementing AI-powered access control solutions, it is essential to understand how user data is collected, stored, and protected, as well as how individuals will be informed about how their data is being used.



Algorithmic Bias and Fairness

AI models are trained on data, and if that data reflects existing biases, the AI can perpetuate or even amplify them. That's why AI-driven access control systems must be trained on representative datasets, so they operate fairly and accurately.

A prominent MIT Sloan School of Management report found that AI often reflects societal biases, including gender and racial disparities.

AI models should be trained on datasets that encompass a diverse range of demographics to prevent biased results. When coupled with regular evaluations to measure disparities in accuracy across different groups, companies can proactively identify and mitigate potential biases, allowing their access control solutions to improve progressively over time.

Transparency and Explainability

When an AI system makes a decision, like denying access, can the reasoning behind that decision be understood and explained? Black-box AI systems can be problematic in sensitive applications; explainability is needed to build trust, ensure accountability, and identify potential errors or biases in the system's logic.

Confidentiality with LLMs

A large language model (LLM) may utilize a company's internal data to train, enabling it to perform tasks more effectively specific to that organization. However, providers of this technology must ensure that company secrets and proprietary information remain confidential.

This is especially important when that data includes people's biometric information.

Ethical AI in Action

Aligning with a standard like ISO 42001 sends a powerful message to organizations implementing AI, particularly in sensitive areas

like security and access control. It demonstrates a proactive commitment to responsible AI governance, moving beyond mere compliance to actively manage the risks associated with AI technologies.

Following these frameworks can help build crucial trust with customers, employees, and regulatory bodies, assuring them that the organization is not only leveraging the power of AI but is also dedicated to its ethical and transparent application. It can also introduce a more formal approach to AI management systems, streamlining internal processes, fostering a culture of accountability, and providing a clear roadmap for improving AI systems.

For C-suite decision-makers tasked with selecting and implementing AI-driven access control solutions, ISO 42001 offers a valuable benchmark.

When evaluating potential vendors, inquiring about their alignment with or certification against this standard can provide significant insight into their commitment to ethical AI development and robust governance practices.

Selecting technology partners who adhere to such standards

can help mitigate potential reputational, legal, and operational risks associated with AI deployment. It also ensures decision-makers and stakeholders that their AI-powered access control solutions are being deployed with integrity, transparency, and intentionality.

The Intelligent Future of Access Control

AI is here. It's reshaping the products we use, the services we rely on, and the processes that improve both over time. It's also reimagining access control solutions in real-time. This can be great news.

AI-driven systems provide enhanced accuracy, predictive capabilities, seamless integration, and a more convenient user experience, all while adapting to the evolving needs of modern enterprises. Even so, the implementation challenges are real as companies strive to balance technological advancements with robust ethical frameworks, transparency, and uncompromising attention to privacy.

Keeping people safe is non-negotiable, as is using the best solutions available to achieve that goal effectively, responsibly, and ethically. **AC**

About the author:



Blaine Frederick serves as the VP of Solutions Engineering at Alcatraz, a global provider of frictionless, AI-powered biometric access control solutions revolutionizing security through facial authentication. In this role, he leads the development and implementation of cutting-edge access control solutions, working closely with customers and partners to drive adoption and innovation.

Frederick brings over 20 years of experience in the Physical Security industry, with specific expertise in the Biometric space. Before his work at Alcatraz, he served as Co-Founder and Principal of BDIS, which provides Consultation and Professional Services for the physical security market. Previously, Frederick served as VP of Product for EyeLock, where he led the firm's vision for iris authentication products and solutions in physical and logical security, as well as numerous other commercial applications.

Frederick also acted as the former Director of Product Management at STANLEY Security, a global division of Stanley Black & Decker, where he led the creation of an industry-leading security management software suite, Commander. He received a B.S. in Electrical Engineering from Purdue University.



Powering the Future of Smart Security



Building a world you can depend on.

As technology shapes the way we live and work, businesses need security solutions that go beyond simple protection – they need solutions that integrate seamlessly and drive results. At Wesco, we make it happen. Our advanced solutions, industry expertise and global partner network help you build a smarter, secure future.

Get in touch with our team.

LockingSolutions@Wesco.com

844.522.5275

Ingenuity delivered.

Wesco.com

241216A003 © 2025 Wesco International





Smart Locks Come of Age

Any discussion about smart locks leads to a broader conversation about mobile access, biometrics, and cloud-based technology.

Smart locking systems are shedding their reputation as expensive tech deadbolts, providing great value beyond the door.

BY PAUL RAGUSA



Once thought of as expensive hi-tech deadbolts, smart locks are now living up to their promise of providing convenience, connectivity and scalability, all while giving security professionals more options to offer at the door, and end users more opportunities to get their return on investment – and then some.

As smart lock manufacturers continue to evolve and offer new and creative retrofit options for facilities looking to upgrade their older mechanical locks, the industry is seeing strong early adoption across many verticals such as education, healthcare and multifamily.

“In 2024, IDEMIA released their access control market report, and it showed for the first time that smart locks, as opposed to a wall reader, are now 51% of the total access market,” says Bill Wood, president, North America, Salto, who points out that much of that growth is in the residential segment, both single-family home and multifamily.

“When we think about where we see adoption today, the top markets are very focused around the end user journey, and they are prioritizing the experience of the cardholder or the credential holder more than any other attribute in their choice or selection of smart locking technology,” he says.

Education, hospitality and multifamily are all embracing smart locks and advanced technology like biometrics to streamline that user experience while providing more control and management capabilities.

“Those three markets all have one thing in common because in some aspects of their businesses, there is some kind of lodging experience behind the scenes,” Wood explains. “On a college campus, it’s student housing, in multifamily residential, it’s the tenant, and in hospitality, it’s the guests at the hotel room. And

we also see great promise in healthcare, which is traditionally very focused around compliance. Still, as the healthcare market is decentralizing away from the hospital setting, the customer journey is becoming more and more important.”

“In 2024, IDEMIA released their access control market report, and it showed for the first time that smart locks, as opposed to a wall reader, are now 51% of the total access market.”



*Bill Wood, president,
North America, Salto.*

Adding Value Beyond the Door

As end users begin to ask for smart locking technology, the added value that a smart lock platform can bring far outweighs any initial investment.

“Some of that value comes across differently in each of the vertical markets,” says Brian Telljohann, director of Product Management, Allegion. “With multifamily, for example, migrating to electronic access control with a credential now provides both enhanced security and convenience. Tenants with the credentials don’t have to worry about losing the brass key, and you can take advantage of additional features that incorporate automation and remote lock management.”

From an audit trail to providing property managers with remote management and control, often through a cloud-based software platform, there is much that can be achieved as smart locking technology continues to evolve.

“You’re adding value and services that come together in a more integrated way, so if you are doing package delivery, or self-touring, or tenant amenities, for example, they are all baked into this enhanced user or tenant experience, which also translates into being able to charge a higher rent,” Telljohann points out. “And that’s why we’re seeing such a nice adoption in that multifamily market and now in the institutional market, as some of the same values apply, but it’s more about scalability and providing credential management security. As you have a large population of users, that could be in the thousands to tens of thousands.”

As key management becomes cumbersome, “credentials and a credential system that’s centrally managed is a lot more elegant and it saves time and convenience for rekeying,” he adds. “In addition, the integration of the access control platform into a building automation system of large commercial buildings has a lot of value as well to the building owner.”

As Wood points out, with the emergence of electronic access control and cloud-based technology, you don’t need any on-premises infrastructure other than an internet connection to make a smart locking system work.

“I like to talk to people about the aluminum storefront door, and that’s something that every locksmith feels and addresses for their customers practically every day,” says Wood, noting that in the past converting that aluminum front door would require long hours, drilling and a disruption to the customer, not to mention any issues that may arise during



Allegion

Credentials have migrated to mobile platforms that make access easier and more secure.

or after the installation process. “Now I can just simply remove a cylinder, put in an electronic cylinder and I still have the same manual functionality, but now I’m doing it with an electronic key instead of a mechanical key and I have an audit,” he explains. “And in about an hour and a half, any good locksmith can convert that aluminum storefront door to a battery-operated one that now has scheduled functions beyond just being a card reader, plus audit. And if you connect that up to what we refer to as an IQ bridge to get it to the Internet, you can have a cloud-based operating system that’s up and running on that single door in less than a couple of hours.”

“Some of that value comes across differently in each of the vertical markets.”



*Brian Telljohann,
director of Product
Management,
Allegion.*

With all this technology being leveraged, a locksmith can save considerable money per door while providing additional value propositions that can help make the

customer stickier and bring in more recurring revenue.

Mobile First Mentality

Any discussion about smart locks leads to a broader conversation about mobile access, biometrics, and cloud-based technology. While there are some barriers to adoption within specific verticals, mobile adoption continues to proliferate in college and university settings, as well as in multifamily and healthcare.

“The benefit of the mobile credential is the convenience, so that is outweighing some of these barriers and allowing people to still pursue and decide to upgrade their hardware when necessary



KANTECH **salto** 
INSPIRED ACCESS

Integration for the Ultimate Security System

One solution. One card. One platform. Total control.

How is Kantech's integration with Salto unique?

Unified Credentialing – One ioSmart card powers the entire solution, simplifying user management and reducing support calls.

Effortless Management – Manage Salto locks directly through Kantech's EntraPass software, reducing complexity and saving time on setup.

Plug-and-Play Compatibility – Hardware and software work together seamlessly, making deployments faster and more reliable.



Contact us at [Kantech.com](https://www.kantech.com)



to obtain that user experience,” says Telljohann. “Universities are a good example, as students expect everything to be on their mobile device.”

Olivia Renaud, Allegion’s group product manager for credentials, agrees that adding mobile credentials when selling locks and readers enhances the overall user experience, while broadening what is possible around the door.

“Inherently, mobile credentials force sites and customers to adapt to a single credential technology,” she explains. “Once a school decides that they want to move toward the mobile journey, it makes it more viable to add additional use cases to their ecosystem, such as electronic locks. Oftentimes, it’s the jumping off point to understand the breadth that mobile credentials can offer and starts customers down that journey to expand their use with physical readers and locks.”

Renaud sees a continued proliferation of mobile credentials. “The existing standards and products (e.g., Mifare Desfire) that are driving transition to mobile today, as well as future standards and products (e.g., Aliro), will continue to drive that transition to mobile, including in places where it may not be viable for symmetric credentials to exist,” she says.

Biometric Adoption

All agree that a natural extension of the smart lock is the potential use of biometrics, with facial recognition leading the charge.

“I certainly do think that biometrics will continue to play a role in the access control environment,” says Telljohann. “Where I see the most growth is in identity management, such as at airports with TSA, where you’re focused on validating your identity. When it comes to access, certainly, there are use cases where biometrics can be handy. I think

“Inherently, mobile credentials force sites and customers to adapt to a single credential technology”



Olivia Renaud, Allegion’s group product manager for credentials.

its benefits are primarily around touchless interactions, and using facial recognition is a high-growth area. And they can be very valuable also for secondary authentication for very high security applications, whether that’s government or sensitive university spaces.”

Wood agrees that the phone and biometrics are critical elements in any modern access environment, either as the credential itself or as a tool to help validate an individual’s identity.

“The idea of eliminating the need for a physical credential from certain applications we see as a real enabler, especially in applications where maybe mobile isn’t the best option or solution or the most applicable credential,” he says. “We’ve launched external to North America our first facial recognition reader because I think in the same way the mobile device has pushed out many of our legacy physical credentials for that convenience factor, face is going to push out some aspect of additional credentials, be it mobile or physical, for the convenience factor of being able to just walk up to an opening, have it recognize and identify you and allow for that seamless entry.”

He continues, “In the mobile world, you can use a trusted identity on the mobile device to transfer the key to the wallet or to an app, and then with this mobile

enrollment in the face ID world, we have the ability of the user to send us their protected identity for use in our platform.”

The Cloud and Beyond

The adoption of cloud-based access control systems, in tandem with smart locking platforms, has accelerated over the past few years.

“Cloud-based access control is something we’ve been talking about for a very long time, but I think one of the things we’re seeing now is there is actual adoption,” says Telljohann. “And so, you are seeing more cloud-based solutions in the market that can be more cost-effective than other solutions that may require on-premises hardware and controllers, for example. And we do see folks demanding a more cost-effective solution, which cloud-based access control can deliver.”

The key to the increased adoption of these new technologies is making them as frictionless as possible, adds Wood.

“And that’s my goal when I think about where we’re trying to take the physical access world,” he says. “We need to get it so that these aren’t super complex solutions that require networking engineers and a software database. We need to make it so that both the technology and the mechanical are as simplified as possible to make that delivery process as efficient as possible for the installer and the user.” **AC**

About the author:



Paul Ragusa is senior editor for Locksmith Ledger International, an Endeavor Business Media Security publication.

pragusa@endeavorb2b.com
www.locksmithledger.com



UNLOCK YOUR BRAND'S POTENTIAL SPONSOR OUR EXCLUSIVE ONLINE EVENT

Targeted Exposure | Expert Insights | Industry Leadership



SCHOOL & CAMPUS SECURITY /SAFETY MONTH

OCTOBER

Reach more than **119,000 school and university decision makers** in our month-long webinar series that features 3 one-hour online webinars and a one-hour virtual Roundtable event.

Limited sponsorship opportunities available – don't miss your chance to align your brand with top-tier security innovation in the campus security marketplace.

OCT. 2 | OCT. 9 | OCT. 15 | OCT. 28

Over 770 Leads Generated Last Year - Become a Sponsor Today!

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





Altronix POE367 360W/277V Input Power Supply/Charger Board

Altronix has expanded its power product line with the new POE367 power supply/charger explicitly designed for 277VAC input environments. The POE367 offers a robust and efficient solution for powering IP devices, integrating with NetWay Spectrum Hardened PoE Switches at remote or industrial locations where high-voltage 277V power is the only option.

The POE367 converts 208–277VAC input into a regulated 54VDC output, delivering up to 360W of continuous power. It offers integrated surge protection, LED indicators, and a built-in charger for sealed lead-acid or gel batteries.

For more information on Altronix, visit <https://www.altronix.com/search/277VAC>.



HID Global Booth 8053

Utilize HID Mobile Access to leverage mobile devices and wearables for seamless access to spaces, systems, and more. This trusted technology not only enhances operational efficiency but also drives digital transformation and sustainability while fostering user engagement. Streamline management with the HID Origo portal.

Contact HID



Centrios Access Control Platform

The Centrios platform is designed to seamlessly integrate a mobile app with smart readers and locks so business owners can quickly and easily manage access for all employees and visitors. Through the app, business owners can grant access to employees or trusted vendors, manage access schedules, view access history reports, and users can unlock with a touch of their phone.

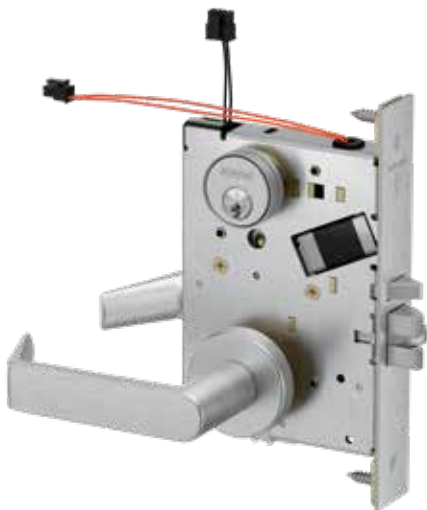
For more information, visit www.centrios.com



Marks USA SKA-Series Indicator Locks

SKA-Series Indicator Locks from Marks USA, a division of NAPCO Security Technologies, provide a clear indication of security status at a glance. Perfect for schools, healthcare facilities, offices, and buildings, they feature bold red and green visual indicators that make it easy for staff, occupants, and security personnel to instantly confirm whether a door is locked or unlocked, providing greater confidence, improved emergency response, and daily peace of mind. Teamed with Marks' durable 5 Series Grade 1 Mortise Locksets, the indicators can be mounted independently or combined on a double-sided basis.

For more information, visit www.marksusa.com



Schlage Latch Retraction Mortise Solutions

Six L Series mortise functions featuring ultra-quiet, motor-driven latch retraction are now available from Schlage. Quick activation can be used for momentary or continuous operation. A unique, patent-pending feature detects binding conditions on the latch motor and adjusts as needed to overcome side load, static pressure and warped door conditions.

Compatible with access control and fire systems, functions include passage, storeroom, institutional and three electrified lever control options. Lever control functions feature a second motor enabling latch retraction and lever control to be managed independently. All functions can be ordered with latchbolt monitoring and all but institutional are also available with request-to-exit. They are offered in all the finishes and lever designs of the L Series and can be retrofitted into the same door pocket.

For more information, visit <https://commercial.schlage.com/en/products/electrified-locks/l-series-motorized-latch-retraction-lock.html>

Salto Systems IQ Mini Gateway

The smallest-ever BLUEnet Wireless peripheral, which is now available in an even smaller device, the Salto IQ Mini combines the best of Salto hardware and software capabilities into a small and versatile design. With advanced BLUEnet wireless technology, it meets the demands of modern cloud-based access control applications.

The small, innovative IQ Mini form factor device of Salto works in tandem with on-device IQ Gateways to help deliver more flexibility and capability. It simplifies network infrastructure while maintaining security and connectivity.

For more information visit Salton at [Salto IQ Mini](#)



CORE WITH CONFIDENCE

A Professional Tool for Professional People

3PCT-300/PDH300 Coring Tool

- Position for coring wood and mineral doors
- Position for coring steel stiffened and foam filled hollow metal doors
- Position for creating mortise pockets for mortise locks, power transfers, flush bolts, etc.
- Can core wide range of doors that have different thickness
- Not affected by warped doors
- Labeled sight lines
- Unlimited coring angle on wood doors, up to twenty degree angle on steel stiffened doors
- Has dual coring heads for coring from both directions
- Cores foam filled steel doors with no debris
- Cores doors mounted in the door frame in the vertical position
- Cores doors in the horizontal position on saw horses
- Bits store inside the tool for easy transport and bit protection
- Easily cores any door width
- Custom made coring bit for deep coring
- Custom made bit for steel door applications
- Custom made two foot long starter bit for a more accurate door penetration



Bulls-I Products

602-370-7209

<http://doorcoringtool.com>

Made in U.S.A. The site is set up for U.S. sales only.



Sielox System Clean Up Utility

Sielox introduced the System Clean Up Utility feature, exclusively available in the Sielox Pinnacle Access Control Platform. The System Clean Up Utility performs a fast and thorough cleanup of invalid or outdated access control data. With Pinnacle's System Clean Up Utility feature, system administrators can identify and address neglected or overlooked access data, such as expired cardholders, duplicate access levels, and inactive cardholders. Current Pinnacle platform users already have access to the System Cleanup Utility feature at no added cost to them.

For more information, visit: <https://sielox.com/its-time-to-spring-clean-your-access-control-system/>



Suprema BioStar Air

Suprema announced the launch of BioStar Air, a cloud-based access control platform designed to support biometric authentication natively. Featuring true zero-on-premise architecture, BioStar Air is designed to secure SMBs, multi-branch companies, and mixed-use buildings.

BioStar Air is built entirely in the cloud. Smart readers with built-in controllers connect directly to the network, with native biometric support by processing biometric data at the edge. The platform's federated architecture enables the use of organization-wide biometric templates. Web and mobile interfaces enable administrators to manage users and devices in real-time from anywhere.

For more information, visit <https://www.supremainc.com>.

Calling all security product innovators!

The 2025 SecurityInfoWatch Readers' Choice Awards are HERE!

Gain exposure by entering the **only** industry product award program that doesn't charge an entry fee.

Winners are determined by reader votes and will be featured online and in *Security Business Magazine*.

Entry takes just a couple of minutes. Don't miss this chance to have your product and brand recognized!

ENTER NOW



www.securityinfowatch.com/readerschoice



THE NEXT LEVEL OF ACCESS CONTROL



X-SERIES HD Video Intercoms

These compact and sleek intercoms offer a feature-rich solution designed to deliver high-definition video and dependable voice communication via SIP VoIP phone systems, cloud providers, or third party apps.

Privacy-focused design with the option for users to choose their own SIP and NVR solutions, giving full control to the end user to host their own systems without the need for forced cloud services or subscriptions.

When you need reliable access control...

YOU NEED A VIKING.



VIKING

715.386.8861
vikingelectronics.com





From the Curb to the Cloud: Lock Up New Business & Revenue

- **From a Few Doors to Many** - Start as simply as using top-rated, low maintenance Trilogy or wireless networked Trilogy Networkx locks on any door- Now All Weatherproof. Then scale from there- Any number of doors, users & credential-types - ALL on choice of numerous platforms, standalone, database, cloud or App.
- **Less to Train/Learn, Trilogy & wireless networked Networkx models feature common familiar operation, programming, & footprint** (most) for every door, user, building and application inside & out - *Easy upgrades- No costly "rip-out & replacements"!*
- **More Revenue Options:** Earn new incremental monthly services revenue from all your Alarm Lock Locks & create happier, more valuable accounts from all your Trilogy & Trilogy Networkx & Designer ArchiTech cylindrical, mortise, exit & narrow-stile locks, at every door & application.
- **More Remote Account Management Options:** Billable, easy security user-, schedule- & door-management services for customers, plus, options for real-time alerts &/or managing access events or lockdown.
- **More Savings from Operating Expenses:** Trilogy is award-winning for its long-battery life, low-maintenance & lowering operational costs + wireless Networkx eliminates door-to-door labor for audits & program updates.



New! MVP EZ Access App-Only, Remote Cloud-Hosted Platform for All Trilogy Networkx Locks & NA-Panels:

Configure, Command & Control All from your Smartphone.

No PC. Scan-n-Enroll Locks, etc. Easy to afford and quote with *One Flat Per-Door Rate*. Full admin controls, lockdown, schedules, emergency SMS occupant alerts and mobile credentials.

More Revenue Starts Here—Free Demo or Class at alarmlock.com/seminars



1.800.ALA.LOCK • www.alarmlock.com

Trilogy, Networkx, ArchiTech and MVP EZ/Access are trademarks of NAPCO.

**Get
Started**

