



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

# SECURITY

Technology | Education | Solutions **today**

May/June 2025 | Vol. 29 No. 2

## HOW LONG UNTIL AI TAKES YOUR JOB?

THE SECURITY INDUSTRY  
AT A CROSSROADS



# 2025 CORVETTE GIVEAWAY

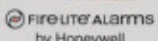
Promo Runs from April 1<sup>st</sup> to November 30<sup>th</sup>, 2025. Drawing in December

## Enter For Your Chance To Win!



# WIN

### OUR SPONSORING VENDORS



To enter, scan the QR code,  
contact your local Security Data Supply  
Team Member for details, or go to  
[www.securitydatasupply.com](http://www.securitydatasupply.com) to register.

The image(s) above are a representation of the prize. The actual prize that will be awarded may vary.

AL Mobile ..... 251.415.3425  
AZ Phoenix ..... 602.900.1969  
ID Boise ..... 208.323.1177  
LA Baton Rouge ..... 225.293.7890  
Bossier City ..... 318.742.8232  
Mandeville ..... 985.674.9890  
Monroe ..... 318.605.2914  
New Orleans ..... 504.836.2040

MO Kansas City ..... 816.834.9111  
NC Raleigh ..... 984.375.3737  
NM Albuquerque ..... 505.888.4000  
OH Cincinnati ..... 513.823.9737  
OR Portland ..... 503.431.2025

TX Dallas ..... 972.416.5020  
Fort Worth ..... 972.416.5020  
Houston ..... 713.782.5100  
Lubbock ..... 806.310.7371  
UT Salt Lake City ..... 801.207.1959  
VA Norfolk ..... 757.260.9040  
WA Spokane ..... 509.624.5943





# FIRE RATED STRIKES THAT DOUBLE YOUR PROFIT!



UL10C/  
CAN4-S104,  
90min. Fire Rating



**1289**

Grade 1 Fire Rated  
Surface Mount RIM Strike  
w/ (1) Latch Monitor

UL10C/  
CAN4-S104,  
90min. Fire Rating



**1689**

Low Profile Grade 1  
Fire Rated Mortise Strike  
w/ (2) Monitor Switches

UL10C/  
CAN4-S104,  
3hr. Fire Rating



**1799**

Grade 1 Fire Rated  
Mortise Strike w/ (3)  
Monitor Switches

UL10C/  
CAN4-S104,  
3hr. Fire Rating



**1410**

Grade 1 Fire Rated  
ANSI Strike

UL10C/  
CAN4-S104,  
3hr. Fire Rating



**NEW!**

**1420**

Low Profile Grade 1  
Fire Rated ANSI Strike

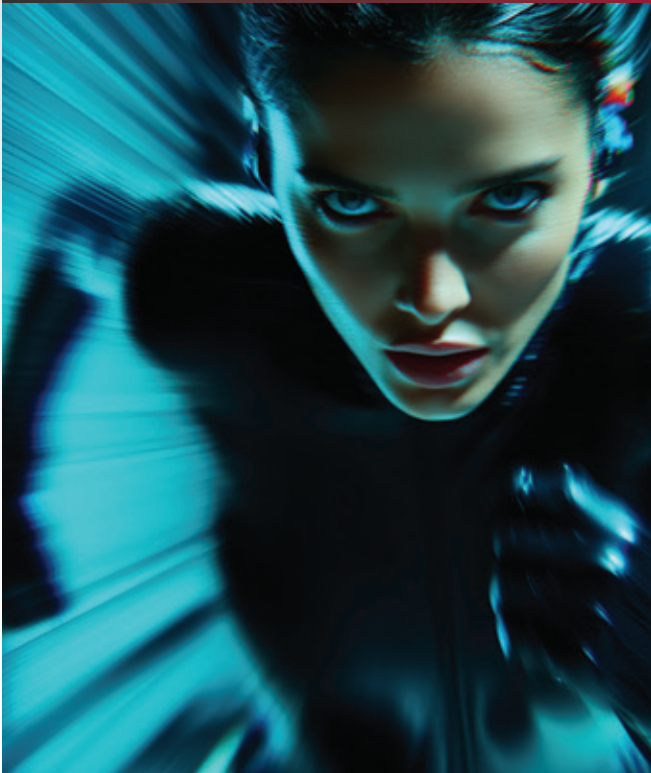
Why pay to stock both UL fire rated and security rated electric strikes? Camden universal strike design supplies a complete list of features, **FREE** latch monitoring, and both fire and security UL listings — all at the best value in the industry!

**Trust Camden for Fire Rated Strike Solutions!**

**LOCKING | CONTROL | ACTIVATION | ACCESS**



### cover story



### How Long Until AI Takes Your Job?

14

The security industry at a crossroads  
By Steve Reinharz



### Cybersecurity 18

**Make Your Metadata Cybersecure**  
How to safely share physical security metadata with your IT systems  
By Wayne Dorris

### Key Management 22

**Facing Facts for Facilities**  
By Craig Newell

### Access Control 24

**Deploying in a Hybrid, Cloud Environment**  
By Kris Houle

### Cybersecurity 26

**The Cybersecurity Time Bomb**  
By Will Knehr

### Smart Buildings 28

**Paving the Way to Smart Buildings**  
By Emma Falck

### features

#### Access Control 8

**Fast-Forward from 1,000 B.C.E. to Today**  
By Peter Boriskin

#### Access Control 10

**Built for Today, Ready for Tomorrow**  
By Charles Nguyen

#### Body Worn 12

**Body-Worn Cameras on the Rise**  
By Alan Ring

### departments

#### Industry Focus 6

**The Forecast is Warm with a Tariff Approaching**  
By Ralph C. Jensen

#### Security Today Solutions 30

#### Advertising Index 33

#### Video Management Systems 34

**A Model for Community Security**  
By Nick Smith

### Online Communities



Follow us on Twitter:

[www.twitter.com/SecurToday](http://www.twitter.com/SecurToday)



Become a fan on Facebook:

[www.facebook.com/SecurToday](http://www.facebook.com/SecurToday)



Link to Us:

<http://llinkedin.com/company/security-today>





## 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™*



With Ralph C. Jensen, Editor-in-Chief



## The Forecast is Warm with a Tariff Approaching

I am going to wade into the weeds for a moment and talk about the current president's plan to tariff the global economy. While leveraging tariffs to achieve parity with unfair trade practices from other nations is understandable. Tariff wars, however, are difficult to deescalate and have significant economic consequences.

The good folks at SIA hit the nail on the head.

"As SIA reviews these policies, we maintain our steadfast view that U.S. trade policy should drive open markets, competitiveness and innovation and effectively protect intellectual property rights. Not only is the U.S. one of the largest security markets, but it also continues to be an important center for product development, intellectual property ownership and manufacturing for many of our members, which are dependent on a global supply chain."

Exactly what does the security industry bring to the global table. We all know that the security industry is grow-



This includes supplier and induced economic activity.

SIA makes its point noticeably clear, "Trade policy should accelerate further growth and contribute to a business climate that thrives as a result of sound, clear and predictable trade policy."

SIA will offer its members analysis of the tariffs, education in different formats and access to experts who can share additional insight into these policies as soon as practical. SIA has your back.

ing rapidly, but the total impact to the economy is \$431.3 billion. According to SIA, the security industry provides 2.1 million jobs, and a payroll of \$145.5 billion in wages.

### ID STATEMENT

*Security Today* (ISSN 2572-5246) is published 5 times a year, Mar/Apr, May/Jun, Jul/Aug, Sept/Oct and Nov/Dec by 1105 Media, Inc., 6300 Canoga Avenue, Suite 1150, Woodland Hills, CA 91367. Periodicals postage paid at Woodland Hills, CA 91367, and at additional mailing offices. Complimentary subscriptions are sent to qualifying subscribers. **Subscription inquiries, back issue requests, and address changes:** Mail to: 1105 Media Inc. c/o Security Today, P.O. Box 291842, Kettering, OH 45429, email [SECmag@sfsdayton.com](mailto:SECmag@sfsdayton.com) or call 800-607-4410 for U.S. and 937-853-2340 for Canada/International. **POSTMASTER:** Send address changes to 1105 Media Inc. c/o Security Today, P.O. Box 291842, Kettering, OH 45429. Canada Publications Mail Agreement No: 40612608. Return Undeliverable Canadian Addresses to Circulation Dept. or XPO Returns: P.O. Box 201, Richmond Hill, ON L4B 4R5, Canada.

### COPYRIGHT STATEMENT

© Copyright 2025 by 1105 Media, Inc. All rights reserved. Printed in the U.S.A. Reproductions in whole or part prohibited except by written permission. Mail requests to "Permissions Editor," c/o *Security Today*, 6300 Canoga Avenue, Suite 1150, Woodland Hills, CA 91367

### LEGAL DISCLAIMER

The information in this magazine has not undergone any formal testing by 1105 Media, Inc. and is distributed without any warranty expressed or implied. Implementation or use of any information contained herein is the reader's sole responsibility. While the information has been reviewed for accuracy,

there is no guarantee that the same or similar results may be achieved in all environments. Technical inaccuracies may result from printing errors and/or new developments in the industry.

### CORPORATE ADDRESS

1105 Media  
6300 Canoga Avenue, Suite 1150  
Woodland Hills, CA 91367  
[www.1105media.com](http://www.1105media.com)

### MEDIA KITS

Direct your Media Kit requests to:  
[www.converge360.com/pages/advertising/sec.aspx](http://www.converge360.com/pages/advertising/sec.aspx)

### REPRINTS

Reprints: For single article reprints (in minimum quantities of 250-500), ePrints, plaques and posters contact:  
PARS International  
Phone: 212-221-9595  
Email: [1105reprints@parsintl.com](mailto:1105reprints@parsintl.com)  
[www.1105Reprints.com](http://www.1105Reprints.com)

### LIST RENTAL

The *Security Today* subscriber list is available for rental. For more information, please contact your Integrated Media Consultant.

Products | Technology | Solutions

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

Volume 29, No. 2

### EDITORIAL STAFF

Editor-in-Chief

Ralph C. Jensen

Editor

Brent Dirks

### ART STAFF

Senior Art Director

Laurie Layman

### PRODUCTION STAFF

Print Media Technician

Joanne Kim

### EDITORIAL ADVISORY BOARD

Pierre Bourgeix, Chief Technology Officer, Founder  
ESI Convergent, LLC

William Crews, President/CEO,  
Security & Resilience Consulting, LLC, Houston

Rob Hile, General Manager,  
Florida GC&E Systems Group, Tampa

Jeff Karpovich, CPP, CHPA, CSSP, Chief/Director, Security &  
Transportation, High Point University, High Point, NC

### SALES

Brian Rendine

972-687-6761

Sam Baird

+44 1883 715 697

### INFRASTRUCTURE SOLUTIONS GROUP

President

Dan LaBianca

Publisher, Security

Ralph C. Jensen

Group Circulation Director

Tillie Carlin

Group Webinar Administrator

Tammy Renne

**1105 MEDIA**  
YOUR GROWTH. OUR BUSINESS.

Chief Executive Officer

Rajeev Kapur

Chief Financial Officer

Sanjay Tanwani

Chief Technology Officer

Erik A. Lindgren

Head of Human Resources

Edie Prince

### REACHING THE STAFF

Contact information is available at [www.securitytoday.com](http://www.securitytoday.com).

**Email:** To email any member of the staff, please use the following form: [FirstInitialLastname@1105media.com](mailto:FirstInitialLastname@1105media.com)

### Corporate Office

weekdays, 8:30 a.m. – 5:30 p.m. PT

818-814-5200

6300 Canoga Avenue, Suite 1150, Woodland Hills, CA 91367





## Perfect Installations and Constant On-Site Promotion

Make a statement, perfect your installations, and continuously promote your company at every installation site!



Customization includes everything you wish for such as material, size, style, color, graphics, studs, standoffs, holes, knockouts, internal panels or racks, windows, clear doors, custom features and more!

**Email us at [info@mierproducts.com](mailto:info@mierproducts.com), or contact your local Mier distributor, to get started!**



**Mier**  
PRODUCTS, INC.



Since 1987

**You name the box, can, cabinet or enclosure: Mier Products has you covered!**

***www.mierproducts.com***

# Fast-Forward from 1,000 B.C.E. to Today

By Peter Boriskin

**T**he lock and key have been around since time immemorial. In fact, the locksmith profession is one of the oldest in the world when you consider the earliest wooden tumbler lock debuted three-plus millennia ago.

Of course, the inventors did not exactly call it an “access control solution” way back then, but the concept was certainly there, at least in nascent form. The idea was to limit who should be allowed to enter so property would be better protected, and its inhabitants would feel safer.

That basic idea remains the foundation of access control to this day. What has changed, obviously, is the technological progress that has been made and the interoperable ingenuity that now helps today’s access control solutions complement and reinforce each other.

## FROM MECHANICAL LOCKS TO INTELLIGENT KEYS, MOBILE CREDENTIALS AND BEYOND

It does not take long to recognize how far we have come from purely mechanical door locks. That is not to say that modern mechanical locks and keys are not still extremely useful and valuable. Take new red button locks on the interior of a growing number of classroom doors that empower a student to activate a deadbolt immediately in the event of a threat.

When you look at the innovation that has occurred in electro-mechanical products, intelligent key systems and digital access solutions, the evolution is impressive and readily apparent. It has yielded, by design, incredible door security benefits.

When the subject of access control comes up, what comes to mind most often are electronic access control (EAC) solutions – particularly those featuring credential readers that activate a door lock once an authorized fob, keycard or mobile phone is presented.

Mobile credentials have become increasingly important everywhere, especially among college-age students considering which schools they apply. They expect their phones to fulfill an expanding range of transactions – from convenient, secure payments for food, bookstore, laundry, and other campus services to easy, safe access to workout facilities, school events, and – most important – campus housing. In fact, mobile access has become a key selling point of higher education institutions.

An exciting, new development in digital access solutions is the deployment of facial identification stations on university campuses and K-12 environments, primarily at openings to athletic workout and event facilities. Because it is a hands-free credential, athletes, coaches, and staff do not have to worry about carrying, stowing or keeping track of a key, fob, card or mobile phone to enter a controlled space.

While mobile devices are excellent and rarely get lost or left behind, a face is something that is always on you. Attractively priced and no longer limited to high-security government applications, facial identification solutions are also gaining interest for other critical environments and applications, including hospitals

and commercial buildings.

Intelligent key systems are also among the EAC solutions that keep gaining momentum. Even though the technology has been around for a while, new applications and beneficial uses keep emerging for these advanced electromechanical cylinders and keys. Efficient to install and authorize, intelligent key and lock systems are ideal for retrofits, providing robust controlled access and physical security while increasing accountability.

## TRAFFIC CABINETS, SMART LOCKERS AND MORE FUTURE-FORWARD ACCESS SOLUTIONS

The solution is also getting more notice as a retrofit for traffic control cabinets that house all the electronics for traffic lights are connected to municipal and statewide networks. Intelligent locks and keys help ensure that only authorized personnel have access, that cabinets are securely closed after equipment is serviced, and that a destructive breach or cyber threat becomes outdated.

Switch locks are another valuable application for intelligent key systems. Being able to program when a certified operator can start and run expensive forklifts, industrial shredders, vehicles and other equipment can help improve both safety and the security of valuable assets.

Key cabinets for securely and reliably storing intelligent keys on site – as well as keeping them charged – are also an essential and practical step for the technology. Key cabinets and key management go a step further by providing audit trails to help keep track of keys, who has access to them, and when.

Assignable and secure smart package delivery and storage locker systems are among some of the other extremely beneficial EAC security solutions now available.

New, intelligent video visitor intercoms with clear two-way communication, HD cameras, and buzz-in features provide yet another layer of electronic access control and are deployed in multi-family housing, K-12, healthcare facilities, and other locations where extra measures to vet visitors are essential.

Digital access has also become more affordable, scalable and practical for small- and medium-sized businesses thanks to unique products and systems designed for that market.

So many of these solutions and applications are seamless, creating an even more high-impact solutions – like mobile credentials and VMS; facial identification and new visitor video intercoms; and intelligent keys and smart locker systems, to name a few.

Thankfully, the use cases keep growing and the innovations keep improving as access control solutions expand to better meet the security and safety needs of more people and places looking to protect lives, living spaces and livelihoods. 📱

*Peter Boriskin is the CTO and senior vice president of ASSA ABLOY Americas.*





# 30 years of innovation. Timeless protection.



Traka was born from the need to help a major airline manage and track keys for its airside ground vehicles. Today, after three decades, our intelligent solutions empower companies to secure, manage, and audit access to critical assets in 25+ industries. With our global reach and local expertise, we provide the security, efficiency, and accountability you need to protect what matters most.

**traka**  
**ASSA ABLOY**

See the impact Traka can have on your business.  
Visit [traka.com](https://traka.com) or see us at GSX Booth #1543.



# Built for Today, Ready for Tomorrow

By Charles Nguyen

**S**electing the right VMS is critical for any organization that depends on video surveillance to ensure safety, security and operational efficiency. While many organizations focus on immediate needs such as budget and deployment size, let us review some of the long-term considerations that can significantly impact a VMS's utility and flexibility.

## OPEN ARCHITECTURE

When selecting a VMS, open architecture is a key factor to consider. Unlike proprietary systems, which can limit device compatibility and stifle future upgrades, an open architecture VMS allows for greater flexibility and adaptability. This enables organizations to integrate various cameras, analytics tools, and other devices, ensuring they can choose the best technologies for their specific needs without being confined to a single vendor.

Closed systems can quickly become obsolete as technology evolves, forcing organizations to either stick with outdated solutions or face the inflated cost of transitioning to a more adaptable solution. When switching to a closed system, businesses may also have to rip and replace their current cameras and other hardware, as these systems often do not support devices from varied brands.

Open architecture VMS platforms support integration with various third-party systems, making it easier for businesses to scale and enhance their surveillance infrastructure as needed. This freedom to choose devices is critical when different sites have varying requirements.

## HYBRID APPROACH

Organizations today often require flexibility in deploying their VMS, especially when dealing with multiple locations or varying site requirements. Hybrid deployments, those that combine on-prem and cloud technologies, offer the best of both worlds.

On-prem servers may provide the processing power and storage needed for larger sites or headquarters. Smaller or remote sites can benefit from fully cloud-hosted systems. Hybrid approaches allow businesses to scale their infrastructure according to their current needs. This gradual modernization ensures that the system can grow alongside the organization, making it easier to integrate modern technologies or expand into cloud services when the time is right.

## RELIABILITY AND UPTIME

Reliability is crucial when choosing a VMS, especially for organizations that consider video surveillance mission critical. Downtime or missed recordings can have profound consequences, from operational disruptions to missed security events.

A VMS with built-in redundancy features such as failover archiving and load balancing helps ensure continuous monitoring, even during hardware or software failures. Combined with automatic resource management, these features can keep systems operational under various conditions, minimizing the risk of losing important video data.

## KEY QUESTIONS TO ASK WHEN CHOOSING A VMS

Does this VMS support a wide range of third-party cameras, sensors, and analytics tools, allowing me to choose the best technologies for my needs?

- Can I gradually modernize my infrastructure and keep my existing investments without disrupting operations or overhauling the entire system?
- Does the VMS include essential cybersecurity tools like encryption, multi-factor authentication, and automated patch management to protect my system from threats?
- How does this system ensure that my organization follows regional privacy regulations?
- Does the VMS offer deployment flexibility, allowing me to choose between on-premises, cloud, or hybrid models based on my specific requirements?
- Can this system easily expand to accommodate more cameras, increased storage, or more technologies like video analytics as my organization grows?
- How does the VMS enable real-time communication and automated workflows to ensure fast response and coordination during security events?
- Can the VMS unify video, access control, ALPR, and other security systems into a single platform, simplifying monitoring and management for my team?

## SCALABILITY AND MOBILITY

As organizations grow, their video surveillance needs will also evolve. A scalable VMS allows for easy expansion, whether adding more cameras, increasing storage capacity, or integrating new technologies such as video analytics or sensors.

Scalability ensures that the organization continues to benefit from its first investment without replacing the entire system as needs change. A good VMS will also offer API or SDK support, enabling custom integrations that extend the system's functionality beyond basic video surveillance.

A modern VMS should provide secure remote access via a web app, allowing users to watch video, manage access control, and quickly respond to alarms with real-time communications from any device with a browser. This ensures better coordination and faster incident resolution.

## CYBERSECURITY AND PRIVACY

As cyber threats become increasingly sophisticated, cybersecurity and data privacy are paramount concerns for any VMS. To mitigate risks, a robust VMS should offer built-in cybersecurity tools such as encryption, multi-factor authentication and automated patch management for both the VMS and video cameras.



Organizations must also consider privacy regulations like GDPR or other regional data protection laws. A good VMS will allow for privacy controls, such as data anonymization and automated video retention policies, to ensure compliance with these regulations.

## UNIFICATION

The terms unification and integration are often used interchangeably, but they don't mean the same thing. Managing and integrating multiple disconnected systems can lead to inefficiencies and security gaps in complex or multi-site organizations. Conversely, a unified platform that centralizes video, access control, and other security systems in a single platform can dramatically simplify monitoring and response activities.

Unified systems offer a comprehensive view of security operations, allowing operators to manage video feeds, alarms, and other security events from one interface. Advanced VMS platforms often come with built-in features like map-based visualization, real-time alerts, native audio capabilities, and mobile access, further enhancing operational efficiency. Unification ensures that critical insights from across the organization are accessible and actionable.

Unification goes beyond security by integrating building systems, IIoT sensors, and business applications into a single platform, unlocking valuable operational insights. A unified platform with intuitive data visualization helps teams optimize space, streamline operations, and improve customer experiences, while also enabling

IT and SecOps to standardize and share data efficiently.

## REAL-TIME CAPABILITIES

Centralized video access allows investigators to easily retrieve, view, and analyze footage from multiple locations in real time. Immediate access to all relevant video feeds, live and recorded in the same view, streamlines the investigation process, enabling faster responses to security incidents.

Smart video analytics enhance this further by automatically identifying critical events, anomalies, or behaviors. These advanced analytics help investigators pinpoint relevant footage quickly, saving time and allowing them to focus on the most important aspects of the investigation. System tools can also ensure that sharing evidence is both seamless and secure, maintaining chain-of-custody protocols while facilitating collaborative investigations.

Choosing the right VMS goes beyond addressing immediate surveillance needs. It's a pivotal decision in building a scalable, resilient security infrastructure. An open architecture VMS ensures adaptability and avoids the constraints of proprietary systems, offering the freedom to integrate the best devices and adopt emerging technologies seamlessly.

*Charles Nguyen is the product marketing manager for Video, Audio, and Analytics at Genetec.*





# ROLLOK

Rolling Doors & Security Shutters

## Certified Security Rated

### Top Choice for Retail and Commercial Security



Spring & Motor Operators Available



Custom Made in the USA



Quality Assurance

**Contact Us Today!**

Phone 888-840-2833 

Website [www.rolllok.com](http://www.rolllok.com) 

# Body-Worn Cameras on the Rise

By Alan Ring



n the evening of Oct. 29, 2024, the owner of 300 Guard based in Houston, was shot while on duty at a convenience store. He returned fire. He was wearing a plated vest and thankfully recovered in the hospital.

The other thing the security guard was wearing that “saved his life” was a body-worn camera. He attributes the camera’s footage to enabling him to establish a clear-cut case for why he returned fire on the suspect, who was arrested that evening, also thanks (Jonathan says) to the footage from the bodycam.

While law enforcement is the best-known use case for bodycams, they are also being adopted more heavily in the private sector, including retail, transportation and private security.

For private security, one of those driving factors is a reduction in police headcount. A First Analysis report from 2023 titled, “Internet of Things: Use of bodycams outside law enforcement set for dramatic rise,” noted full-time sworn-officer headcount had – at the time – had declined for three consecutive years. Private security is being tapped as a first line of defense, and by 2021, the number of security guards nationally outstripped the number of police officers, according to an article in Governing.com.

Another factor behind the rise of bodycams in the private sector is the need for increased accountability, improved safety and transparency in work environments that are considered high risk. And yes, that includes places like retail stores where 80% of frontline retail workers said they feel unsafe on the job, according to a 2024 survey by Axonify. That finding comes as customer incivility is on the rise, making frontline teams the first line of defense in managing unruly or unlawful customers.

The use of body-worn cameras in the private sector is still in somewhat early stages, but the technology has already proven beneficial in these ways:

## DE-ESCALATING AND RESOLVING CONFLICT

Bodycams have the potential to de-escalate volatile situations and aid impactfully with conflict resolution. It is often true that simply the presence of a camera can deter unlawful behavior. When that is not the case, security staff wearing bodycams are trained to defuse challenging situations with strategic de-escalation techniques.

Further, that footage becomes a valuable training tool for handling similar situations in the future. It can be used to analyze interactions and help improve guard performance in challenging scenarios.

Body-worn camera footage provides an objective account of the events leading up to an incident, if one still occurs, which helps with the impartial resolution of disputes.

## ENHANCING DATA SECURITY AND PRIVACY

Despite the benefits of bodycams, they also raise data security and privacy considerations that must be addressed. Private security firms and others deploying the cameras should have strict

protocols for safeguarding video footage and ensuring compliance with relevant privacy regulations. This can cover everything from data retention policies to encryption to the confidentiality of video footage.

This is where the value in having both the bodycam hardware, and a secure data platform comes in. Users can ensure footage is encrypted on the camera and uploaded directly and securely to the platform. They can manage user permissions to limit who can access the data, ensuring it is safeguarded, backed-up and ready for easy retrieval by only the appropriate parties when needed.

Body-worn cameras serve as the eyes and ears of security staff and increasingly – frontline teams – providing a first-person perspective of what is happening around them. The devices are outfitted with high-def cameras and audio recording capabilities, making them a critical tool for capturing information as incidents unfold. Whether patrolling a crowded venue or managing a disturbance on public transit, the technology arms the wearer with invaluable situational awareness. This helps them assess threats and respond in the best way possible.

Another benefit of bodycams is the ability to livestream, allowing teams on the ground to relay real-time footage from multiple viewpoints to off-site monitors who can help coordinate response efforts. Having an unfiltered, comprehensive view of the environment enables personnel to anticipate and address security concerns quickly and smoothly.

Deploying body-worn cameras can encourage a culture of transparency for the user whether a security firm, retailer, transportation provider or beyond. Recording interactions between personnel and customers promotes adherence both to ethical conduct and professional standards, and it helps resolve conflicting “he-said/she-said” accounts protecting the employee every bit as much as the patron of an establishment.

Beyond their operational benefits, bodycams are a valuable training and professional development tool. Footage can be used for post-incident analysis and debriefing, allowing security personnel to review and reflect on their actions and identify ways to improve. This, in turn, fosters a culture of continuous learning and improvement.

Bodycam footage can also be incorporated into training programs whereby it provides real examples of security protocols and best practices. By immersing trainees in scenarios based on actual incidents, teams can use the footage for experiential learning and enhance the proficiency of their employees.

Do not be surprised next time you are in a store and see the checkout clerk wearing a bodycam. Same goes for riding the train and observing transit staff outfitted with the cameras. 📹



*Alan Ring is CEO of HALOS Body Cameras.*





# Security's Fastest Team Member Isn't Human

**No bias. No burnout. Just results.**

Built with Agentic AI, SARA responds faster than any human. She doesn't assist your team, she becomes it.

Meet SARA, the Speaking Autonomous Responsive Agent.

She monitors live video in real time, identifies threats instantly, delivers authoritative voice-downs, and escalates when it matters most.

No coffee breaks. No attention lapses. No second guesses.

Traditional monitoring teams miss up to 95% of incidents after just 20 minutes. SARA doesn't.

## SARA™

**Start Watching  
Start Responding**

[radsecurity.com/sara](https://radsecurity.com/sara)  
877.78.ROBOT



# How Long Until AI Takes Your Job?

The security industry at a crossroads  
By Steve Reinharz



**T**he security industry is facing a transformation unlike any in its history. Indeed, much of the modern world is in this position. From the industrial revolution to the rise of automation, labor-intensive roles have continuously evolved, and security is no exception. AI is now fundamentally altering how security is managed, shifting from human-reliant surveillance and guard services to intelligent, autonomous security solutions.

This shift raises a critical question: How long until AI takes over traditional security jobs?

Short answer: It has already begun. And While AI will undoubtedly replace many roles, the reality is more complex. The security industry is not being eliminated; it is being redefined, again much like many other global industries. Those who embrace this evolution will find new opportunities, while those who resist risk being left behind. As with every revolution there will be winners and losers.

But you are reading this because the headline touched a nerve, and you want to calculate the reality of Your job being at risk – and when. Read on for answers.

## THE LIMITATIONS OF TRADITIONAL SECURITY

For decades, security has depended on human staffing and reactive surveillance systems. Security officers patrol sites, respond to incidents, and monitor surveillance feeds. However, these legacy models come with significant challenges.

**Human attention span limitations.** Studies show that after 20 minutes of continuous monitoring, an operator's ability to detect threats drops by up to 95 percent.

**High labor costs.** Security staffing requires significant investment in wages, training, and scheduling, making 24/7 coverage expensive.

**Reactive rather than proactive.** Surveillance systems often serve forensic purposes rather than preventing incidents in real-time.

**Inconsistencies in human response.** Security staff may experience fatigue, distraction, or gaps in coverage, leading to missed threats.

The flaws of this system are well documented. Former FBI Special Agent and RAD's chief security officer, Troy McCanna, witnessed these failures firsthand.

"We had a GSOC at the FBI with two people overseeing 300 camera feeds," McCanna said. "They didn't even glance at them. Footage was only reviewed after something happened. There was no proactive monitoring because it just was not possible."

Security companies are now recognizing that human-led monitoring and patrols alone are no longer enough. AI is stepping in to fill these gaps.

## THE REMOTE VIDEO MONITORING REVOLUTION

One of the security industry's largest and most immediate shifts is happening in Remote Video Monitoring (RVM). Traditionally, remote monitoring has relied on human operators watching dozens of live feeds simultaneously, attempting to identify security threats in real time. This model is proving increasingly inefficient for several reasons.

**Cognitive overload.** Security operators monitoring multiple

screens experience fatigue and reduced effectiveness.

**Missed events.** Many critical incidents go unnoticed because human operators cannot sustain constant vigilance.

**Slow response times.** When a threat is detected, the manual reporting process delays intervention.

**High operational costs** – Maintaining 24/7 monitoring teams is expensive and difficult to scale.

AI-powered solutions are disrupting this space by replacing human oversight with intelligent, autonomous monitoring systems. AI-driven monitoring platforms like RAD's SARA™ (Speaking Autonomous Responsive Agent) are revolutionizing RVM by analyzing and responding to video feeds in real time, without requiring continuous human intervention.

## HOW AI IS TRANSFORMING REMOTE VIDEO MONITORING

**Real-time threat detection.** AI-powered platforms monitor live feeds with unmatched accuracy, detecting unauthorized access, suspicious movement and anomalies instantly. AI does not experience fatigue or distractions, ensuring consistent, 24/7 surveillance.

**Automated response and engagement.** Unlike passive camera feeds, AI actively engages with potential threats by issuing audio warnings, flashing deterrent lights, and escalating alerts to security teams. AI-driven monitoring can differentiate between routine activity and real threats, reducing false alarms and unnecessary security dispatches.

**Cloud-based scalability.** AI-enabled remote monitoring allows video feeds to be processed in the cloud, enabling security operations centers to scale without increasing staffing costs. Security teams can oversee multiple sites efficiently, shifting from direct monitoring to managing AI-generated alerts.

**Cost reduction and efficiency gains.** AI automates tasks traditionally managed by human operators, significantly reducing operational costs. Organizations transitioning to AI-driven monitoring can reduce reliance on large monitoring teams while improving overall security outcomes.

McCanna emphasizes the impact of this transformation: "The era of relying on people to stare at screens for hours hoping to catch something is over. AI-powered monitoring like SARA sees everything, responds instantly, and ensures security threats do not go unnoticed."

## THE SARA AI AGENT: REDEFINING SECURITY COORDINATION AND RESPONSE

The introduction of AI-powered security agents has transformed the way incidents are detected, assessed, and addressed in real time. RAD's SARA (Speaking Autonomous Responsive Agent) represents a fundamental leap forward, replacing outdated, fragmented security processes with an intelligent, fully integrated AI-driven command center that operates faster and more efficiently than human-led monitoring ever could.

**A live information transfer hub.** SARA acts as a real-time communication bridge, engaging with multiple parties simultaneously to streamline incident response. Whether coordinating between on-site security, remote monitoring centers, or emergency response

ers, SARA ensures critical information flows instantly between the right people. By keeping multiple stakeholders informed at once, SARA eliminates delays, prevents miscommunication, and enables the fastest possible response to security events.

**Comprehensive situational awareness.** Unlike traditional security operators who are limited by attention span and screen count, SARA monitors all available camera feeds at the same time. This continuous, multi-angle oversight ensures no event goes undetected, providing designated security personnel with instant insights on what is happening and where. The result is unmatched awareness, faster decision-making, and proactive rather than reactive security management.

**Real-time video sharing on demand.** When an incident occurs, security professionals need immediate visual confirmation. SARA eliminates delays by sending live video feeds via text message, giving security teams, law enforcement, or authorized stakeholders instant access to critical footage. Whether assessing a potential intrusion or verifying a situation remotely, SARA puts real-time intelligence directly into the hands of decision-makers.

**Autonomous security deployment.** Beyond detection and communication, SARA takes action. The AI agent can dispatch instructions to other autonomous security devices such as robotic patrol units and deterrent systems to respond to incidents in real time. Rather than waiting for human intervention, SARA ensures that security assets are deployed immediately, reducing response time and minimizing risk.

This level of intelligent automation fundamentally changes what is possible in security operations. By eliminating human bottlenecks, increasing situational awareness and enabling seamless coordination between monitoring, response teams, and autonomous devices, SARA delivers performance, efficiency, and cost savings that legacy security systems simply cannot match.

## AI-POWERED SECURITY GUARD AUGMENTATION

Beyond remote monitoring, AI and robotics are supplementing traditional security staff in other ways.

**Autonomous patrol units** conduct mobile surveillance, reducing the need for on-site guards.

**AI-powered access control** verifies identities and manages site entry without human oversight.

**Predictive security analytics** identify risks before incidents occur, enabling proactive security measures.

“AI-driven security isn’t about eliminating jobs; it’s about elevating them,” said Mark Folmer, CPP, PSP, president of Robotic Assistance Devices. “Security professionals will move from passive monitoring to managing, analyzing, and responding with greater precision.”

## INDUSTRIES ALREADY MAKING THE SHIFT

AI-powered security is no longer theoretical—it is actively replacing outdated models across multiple industries.

**Corporate campuses.** AI security units provide autonomous patrols, facial recognition access control, and real-time security alerts.

**Retail centers.** Automated security towers detect loitering,

trespassing, and suspicious activity, issuing immediate deterrent responses.

**Construction sites.** AI-powered mobile security trailers protect expensive equipment and materials from theft and vandalism.

**Healthcare and critical infrastructure.** AI-driven monitoring solutions safeguard hospitals, data centers, and power plants from intrusions.

These advancements are setting a new standard for security, making traditional models obsolete. Organizations that fail to adapt to AI-driven security solutions will face increased costs, higher risks, and competitive disadvantages.

## THE ROLE OF HUMANS IN AI-POWERED SECURITY

Despite AI’s growing role, security professionals are not being entirely replaced. Instead, their roles are shifting toward oversight, management and high-level decision-making. AI manages repetitive, mundane security tasks, allowing human staff to focus.

**Interpreting AI-generated insights.** Security officers analyze AI-driven threat assessments and determine appropriate responses.

**Managing AI security systems.** Staff oversee AI-monitored facilities, ensuring compliance and effectiveness.

**Providing hands-on intervention.** While AI monitors and alerts, human officers intervene in high-stakes security incidents.

McCanna sees this shift as inevitable: “Security leaders need to make a choice. Stick with failing systems or move forward with AI-powered monitoring. The ones that choose AI will come out ahead.”

## THE SECURITY INDUSTRY’S FUTURE

The integration of AI into security is not a passing trend; it is the future. Security firms and professionals who resist this shift will find themselves unable to compete with AI-enhanced competitors offering better coverage at lower costs.

As AI adoption accelerates, companies should have questions.

- Are we prepared to integrate AI into our security operations?
- Are we equipping our workforce with the skills to manage AI-driven security systems?
- Are we investing in the right technologies to stay ahead of industry changes?

Those who answer “no” risk falling behind in a rapidly evolving industry.

The security industry is at an inflection point. AI is not replacing security; it is redefining it. Remote Video Monitoring is the first sector experiencing widespread AI adoption, and other areas of security are following quickly. Companies that embrace AI-driven solutions will lead the way, while those that ignore this shift will struggle to stay relevant. The question is no longer if AI will take over traditional security roles, but when. And for many, the answer is now. 🤖

*Steve Reinharz is the founder and CEO/CTO of Robotic Assistance Devices, Inc. (RAD) a wholly owned subsidiary of Artificial Intelligence Technology Solutions, Inc. (trading ticker \$AITX).*







ASSA ABLOY

Advanced  
Monitoring  
Options

Retrofit-Ready  
Designs



Preload  
Capable  
Designs

Third-Party  
Certified  
Strength &  
Durability

Simplified  
Installation  
Templates

Flexible  
Mounting &  
Adjustment

Complete  
Pac: One  
Box Solution

Architectural  
Finish Options

Modular  
Faceplates  
& Mounting  
Hardware



Widest  
Range of  
Applications

# More Features. More Options. More Possibilities.

## Designed to Do More, So You Can Too.

We don't just meet industry standards—we exceed them.

**Our features give you more options**, delivering the flexibility to secure any opening. Choose from **advanced monitoring**, **durable finishes**, **preload solutions**, and **third-party certification testing** to ensure reliability where it matters most. When you need more from your access control, **we deliver possibilities.**

*Every Lockset. Every Application.*

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

Experience a safer  
and more open world

# Make Your Metadata Cybersecure

How to safely share physical security metadata with your IT systems

By Wayne Dorris

**W**e all know that physical security devices capture a massive amount of information about the environment in which they're deployed. When categorized and searched efficiently, that data transforms into actionable intelligence to better protect the organization. That is where metadata comes into play.

Metadata is often generated in conjunction with a digital file – be it a video image, a sensor reading, or a sound wave – to describe the file and its contents.

For example, a digital image file may include metadata like the date and time the image was captured, its location, as well as the camera ID and settings used. The metadata can also include details such as the type of object (vehicle, person, animal, etc.), its size, how fast it is moving, even the direction of its movement. In essence, the metadata provides a table of contents for the data to simplify the process of understanding, sorting, and locating the data it represents.

## BUSINESS INTELLIGENCE

With metadata multiple stakeholders can extract different business intelligence from the same data source. For example, a security camera can read license plates to bar unauthorized vehicles from entering a restricted parking facility. It can also count cars, compare that number to garage capacity, and automatically trigger electric signage directing vehicles to an overflow parking lot.

It might be a security camera that watches a fire exit to prevent illegal usage can also alert on detecting a blocked exit, enabling the organization to avoid fire code violations and costly fines. Or security cameras observing for theft at a construction site can also be used to detect whether construction workers are wearing their personal protection equipment as OSHA requires.

It is the metadata that makes it possible for security camera data to contribute to op-



alexskopje/stock.adobe.com

erational efficiency and inform pivotal business decisions. For instance, cameras could confirm QA/QC activity on a production line to help reduce costly waste or frequent remakes. Or the data they collect could help the company find events affecting workflow and operation uptime, which in an industry like automotive or circuit board manufacturing could save millions of dollars in lost production time and help management figure out ways to increase output.

While this might seem like an ideal synergy – using the same device to channel critical insights to multiple stakeholders – it raises significant concerns about the safety and integrity of data flowing between systems.

## BECOMING A TARGET FOR INFILTRATING CRITICAL SYSTEMS

Once security cameras primarily designed for physical security tasks start streaming data and metadata to enterprise operational and business systems, it increases their visibility. Instead of being largely ignored by hackers, they suddenly become high-value targets that can be used to infiltrate and bring down vital production and business operations.

In the past, physical security solutions operated on their own independent networks. Or IT sequestered the physical

security system in a separate zone on the network, isolating it from any critical business and production functions. These decisions were made because IT did not trust that the cybersecurity measures on those devices were up to IT standards.

## WHAT IT EXPECTS FROM DEVICES ON ITS NETWORK

For many physical security system manufacturers, software developers and users, IT-level cybersecurity is a new ball game. To play in IT's sandbox, physical security devices will need things like:

- Multilayer encryption
- Certificate protocols
- Zero-trust architecture
- Automated onboarding and provisioning
- Active Directory and Single sign-on
- Lifecycle management

These are not new security protocols. They have been standard requirements in IT systems for more than a decade. But many are new to physical security devices.

## UNDERSTANDING THESE SECURITY PROTOCOLS

IT security protocols serve two purposes: protecting the integrity of systems and data and making it easier to manage the devices on the network.



# Drive-Alert Vehicle Detection and Asset Protection Systems

Detect approaching vehicles or movement of your equipment



## Off-Grid or On-Grid, Wireless or Hard Wired...

- **FREE** sales & tech support for help choosing the perfect system for your installation
- Accessories to activate sound and/or lights in any room, outdoors, or other buildings
- Extra contacts to easily activate NVRs, gates, signs, alarm panels, etc. (DA-700 & DA-500)
- Choice of different chime tone alerts for different zones, or driveways
- Choice of different styles of sensors: wireless, buried sensor, or hybrid buried and wireless
- Wireless detection up to 1000 feet away, or up to 3/4-mile with our reception booster accessory
- Use our repeater to jump the alert to other areas or buildings up to 1000 feet away
- Use unlimited number or combination of control panels, chimes, lights, repeaters, or sensors
- All interior control panels can be powered by +24 VDC through the J1 input jack using the included DA-050 wall transformer or regulated DC bus via a 5.5mm x 2.1mm DC Power Barrel Plug.

### DA-100 Wireless System

Simple system with volume controlled chime.



### DA-700 Wireless System

Easily installed with volume controlled chime, and extra relay dry contacts to activate ancillary equipment and other alerts



### DA-500 Buried-Sensor System

Perfect for off-grid use with volume controlled chime, and extra relay dry contacts to activate ancillary equipment and other alerts.

Single point +24VDC power on this system, with no batteries to replace.



## Contact Mier Products for more information

[www.mierproducts.com](http://www.mierproducts.com) | [info@mierproducts.com](mailto:info@mierproducts.com) | 800-473-0213



Proudly Made in the USA



“In addition to protecting network access, zero-trust architecture enables IT to automate device enrollment, which, depending on the number of security devices being introduced to the network, can be a critical time saver.”

**Multilayer encryption.** While most physical security devices can encrypt data, IT security protocols take encryption to the next level. Employing multiple encryption layers and multiple encryption keys makes it more difficult for malicious attackers to gain access to the data stream. For example, MACsec encryption might be used at layer two for services like DHCP, NTP and ARP while HTTPS might be used at layer seven for API calls and WebGUI.

**Certificate management.** Many security devices employ certificates, digital documents that verify a device's identity on the network and mechanisms for encryption used to transmit its data. However most physical security devices don't support certificate management protocols like EST (Enrollment over Secure Transport) or SCEP (Simple Certificate Enrollment Protocol). These protocols automate the process of installing and replacing device certificates. Since certificates are crucial for encryption and authentication, it is unlikely that IT would approve devices that require manual certificate management.

**Zero-trust architecture.** IT relies on zero-trust architecture to minimize the radius of damage should a breach occur. This entails micro-segmenting sensitive resources, using end-to-end encryption, continuously monitoring user and device behavior for anomalies, and implementing robust incident response and recovery mechanisms. To support that goal, IT needs to be able to verify the authenticity of physical security devices before authorizing their access to the network.

In addition to protecting network access, zero-trust architecture enables IT to automate device enrollment, which, depending on the number of security devices being introduced to the network, can be a critical time saver.

That is why IT wants security devices that can be onboarded and provisioned automatically through secure network protocols. For instance, devices that use device IDs or 802.1 AR can be loaded onto the network automatically, right out of the box. Once installed, the policy engine server on the network checks the device's ID and associated policies like which ports to open, and so forth.

So, the IT administrator doesn't have to touch the device or assign it an IP address or a VLAN. To simplify things further while on a provisional VLAN device, IT can harden the security device with management software.

**Active directory and single sign-on.** In physical security systems, administrators tend to manage user privileges in local accounts. But in an enterprise environment, IT security protocols require that network devices be managed more securely through a

centralized user rights management service like Active Directory.

To operate in this global enterprise domain, physical security devices would need to support protocols like OAuth 2.0, an IT industry standard for authorization. This would allow the physical security device to be managed more efficiently, like how servers and other IoT devices are managed on the IT network.

For instance, with Active Directory, HR could delete a resigning security officer from the Active Directory, which would automatically revoke their access privileges for all devices across the entire network at once.

Working with Active Directory also allows security devices to support Single sign-on, an authentication service that allows users to log in once to access multiple services without re-entering their user ID and password. This also allows IT to activate more secure authentication features like 2FA, or MFA on these devices, adding another layer of network protection.


**Lifecycle management.** Because cybersecurity risks exist at every stage of a device's lifecycle, IT needs to be able to manage the security of every device on the network from the time it is onboarded until it is decommissioned and removed. IT will be looking for security devices that support features like secure boot, which ensures that the device is free of unauthorized software modifications prior to connecting to the network.

They will also want to be able to batch process security tasks like security patches, bug fixes, and upgrades to device operating systems. In addition, IT will want devices that allow them to easily manage device credentials, deploy certificates, disable unused services, and verify removal of outdated devices no longer supported by their manufacturers, which, unless detached, could become potential attack vectors.

Can these security protocols be retrofitted to legacy physical security devices? In most cases, the answer is no. One might be able to retrofit certificate management like EST or SCAP, but not zero-trust features. Things like a device's digital identities need to be baked into the product at the start for it to be trusted. If security device manufacturers plan to follow these more stringent requirements, they'll need to revamp their production process.

## INVESTING IN CROSS-BREACH PREVENTION

As more stakeholders avail themselves of physical security metadata for business intelligence and operational efficiency, opportunities increase for organizations to identify ways to improve their bottom line. But using that data stream also increases the visibility of physical security devices, making them tempting targets for attackers to exploit.

Without IT-level security protocols on these devices, the potential for a breach into critical IT systems can escalate. On the other hand, having these protocols in place not only helps prevent system corruption and operation disruption, but it also assures the integrity and authenticity of the data being shared. 

*Wayne Dorris, CISSP, is the program manager for cybersecurity for Axis Communications in the Americas.*





# They'll Never Have to Guess Who's at the Gate Again

With a **New Camera & Soft Light Glow**  
The 2112 Video Entry System Delivers a  
Clear Picture of Visitors Day or Night



Introducing the improved DKS 2112 Video Entry System — now with a view that's not too dark and not too light *but just right*. With a powerful camera and enhanced ISO sensitivity, you'll get a crystal-clear, detailed image... even in the darkest forest. The Soft Light Glow of the keys and call button ensures your visitors are always illuminated — no more pawing around in the dark or getting startled by a harsh light. Whether it's a late-night delivery or a surprise visitor, the DKS 2112 makes sure you're not "bearly" seeing who's at the door.



**2112**  
Single Family Entry System



Control Up to 3  
Entry Points



Ring 4 Phones  
Simultaneously



Browser  
Programming



Voice & Video  
Communication



Ethernet or Cellular  
Connection



doorking.com/2112-evolve  
800-673-3299 • info@doorking.com



# Facing Facts for Facilities

By Craig Newell

**D**espite the proliferation of constantly evolving security solutions, there remains a troubling trend among many facility operators who often neglect the most important security assets within their organization. Keys and shared devices like radios, laptops and tablets are crucial to successful operations, yet many operators are managing them haphazardly through outdated storage systems like pegboards and notebooks.

Not only does this represent a security threat if a key or device goes missing or ends up in the wrong person's hands, but a financial risk as well, should that device need to be replaced, or a facility needs to be re-keyed. Fortunately, solutions exist to proactively address these risks and help facility operators safeguard their buildings.

Regardless of the size of a facility, there are inevitably differing access levels required for various staff. This is especially the case in shared space facilities that have multiple tenants.

Building operators, therefore, must institute some measure of intelligent key management, which includes modern key cabinets that integrate into the building's access control system and are programmed so that only certain staff can access designated keys. The cabinet safely stores shared keys to a variety of areas like server rooms, maintenance closets, security headquarters, food and beverage.

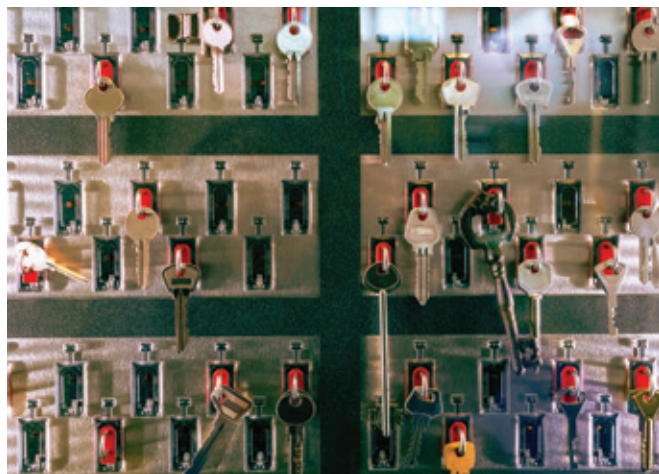
By keeping keys in a strategic location that is monitored through an integrated system, operators have comprehensive insight into who has access to which key and when it was last checked out. Keys are assigned curfews so that if they're not returned by a specific time, an operator is notified, which helps identify when a key may be lost and cuts down on the time spent looking for it.

For larger facilities, multiple cabinets are implemented at strategic locations, thereby eliminating the need for users to travel from one part of the facility to the other for a key. Managers can remotely monitor key usage from a central location, which allows them to reassign staff who were previously assigned to check out keys to another task within the facility. Key cabinets are also critical to producing audit reports for compliance purposes, as they prove who had access to which area and when.

Many of the same principles that apply to key cabinets are seen in intelligent asset management lockers, which store vital shared devices. These modular lockers are important to operations as they ensure radios, tablets and laptops are safe and accounted for, which extends their usage. Modern lockers include charging capabilities so that when a user checks out a device, the system will prioritize the most charged asset, which cuts down on the possibility of mistakenly taking a dead device.

If there is an issue with the device, a user notes it in the locker interface, which removes it from circulation until it has been corrected. Just like with keys, if an asset is not returned by a certain time, an operator is notified and can check the system to see who had the asset last.

While modular asset management lockers are typically for more permanent assets, there has been a growing interest among facility operators for temporary deposit lockers, particularly in



Grispb/stock.adobe.com

**"By keeping keys in a strategic location that is monitored through an integrated system, operators have comprehensive insight into who has access to which key and when it was last checked out."**

shared environments. For instance, if a tenant or vendor needs to use a piece of equipment like a hard drive and the building operator wants to store it separately from internally used shared devices, it can be kept in a temporary storage locker.

Operators can assign access to a user for a certain time, which safeguards unauthorized access to that shared piece of equipment and maintains a clear audit trail of usage.

Despite the clear advantages of key cabinets and asset management lockers, many facility operators are hesitant to shift to more modern solutions in defense of standard operating procedures that they perceive to be failproof. Because security threats are constantly changing, it is important that solutions — and subsequent processes — advance in parallel to protect facilities and staff.

Moreover, it is critical that solutions integrate with existing access control platforms so that onboarding employees to them is seamless and access is activated or deactivated comprehensively through a single credential.

It is worth noting that implementing these smart solutions should be foundational for new facility construction, which is only expected to increase in the United States. By incorporating smart solutions from day one, operators send a clear message to staff that they are taking security and operations seriously and that they have invested in the people who conduct meaningful business inside their walls every day. 📧

**Craig Newell** is the vice president of Sales and Business Development at Traka Americas.







# THEY ALL HAVE ONE THING IN COMMON

**Locks tend to stay put. People don't. The more keys you issue, the bigger the burden in tracking their ownership and use.** What you need is a networked solution that automatically accounts for every lock and key you are charged with managing. CyberLock achieves this through an advanced lock/key technology paired with software that controls virtually every aspect of key ownership and usage.

**CyberLock has over 400 intelligent locks to choose from.** You can simply replace the cylinders in your existing mechanical locks with our intelligent ones. To network your solution, we offer a series of communicators that interface with your local network or cellular device. Our CyberAudit software allows you to track ownership, follow audit trails, deactivate lost keys, and set access schedules. And this is just the start!

So give all your keys and locks something in common through our integrated hardware and networked software. **Contact us today!**

# Deploying in a Hybrid, Cloud Environment

By Kris Houle

**T**he way organizations manage access control is evolving. Traditional on-premises systems come with high IT and server requirements. At the same time, fully cloud-based solutions may not meet the needs of every facility.

Hybrid-cloud access control bridges the gap, giving businesses the best of both worlds—combining on-prem infrastructure with the flexibility of cloud-based management. As companies embrace multi-site security management and cost-saving initiatives, hybrid-cloud access control is becoming the model of choice.

Many businesses are shifting toward subscription-based models for cloud services, reducing the financial strain of major server and IT infrastructure investments. Hybrid-cloud access control enables businesses to modernize security systems at their own pace. While cloud services follow an operational expense (OpEx) model, hybrid solutions often retain a mix of OpEx and capital expense (CapEx), allowing organizations to balance upfront investments with recurring costs based on their financial strategy.

For security, flexibility, and scalability, hybrid-cloud access control is the ideal solution for most organizations. By combining on-prem security with cloud capabilities, businesses can modernize systems at their own pace.

## ADAPTING TO A CHANGING WORLD

Cloud options for video management began years ago. Security and IT teams who experienced the flexibility and ease of remote management for video began to want the same benefits for access control. However, there was not a strong drive to invest in replacing legacy systems. Access control is capital-heavy, with a lot of hardware.

A hybrid-cloud model changes that equation. It allows businesses to modernize security infrastructure to take advantage of the most important benefits of cloud technologies without having to rip and replace an entire existing system.

Leveraging cloud services can also reduce the burden on IT teams to maintain infrastructure. In a traditional on-prem system, troubleshooting, system setup and commissioning needs to be done at a local level. This is especially the case when managing multiple locations and multiple systems with a complex architecture. Cloud solutions simplify this.

With hybrid-cloud, security teams can update access permissions across multiple locations from anywhere, reducing response times and improving efficiency. Automatic updates are pushed to the system to keep it secure and compliant with evolving industry standards, which frees IT teams to focus on more important tasks.

There's a common perception that cloud security is weaker than on-prem, but in reality, leading cloud providers invest heavily in cybersecurity, offering real-time monitoring, encryption and automated patching. In highly regulated industries, a hybrid-cloud model can provide enhanced security by allowing businesses to retain local control over sensitive data while leveraging

cloud-based analytics and automation.

On-prem, cloud, and hybrid deployment models each have their place. None is intrinsically 'better' than another. Work with your systems integrator to consider factors like compliance requirements, remote access needs, and availability of resources. Then choose the model that is best suited to your situation.

A hybrid-cloud access control model is practical for most organizations because it provides the flexibility to choose what stays on-prem and what moves to the cloud. For example, many organizations manage critical security devices, such as door controllers and badge readers, locally. User management, monitoring, and analytics may be moved to the cloud for efficiency.

Here are a few things to consider when selecting deployment options.

**Easy of use and remote management.** When choosing a hybrid-cloud access control system, ease of use and remote management should be top priorities. With the latest cloud-managed solutions, IT teams no longer need to be on-site for every update or maintenance task.

**Difference between IaaS and SaaS.** When evaluating cloud access control solutions, it is important to distinguish between infrastructure as a service (IaaS) and software as a service (SaaS). IaaS solutions host access control software in the cloud, but businesses remain responsible for managing configurations, updates and security. SaaS, on the other hand, eliminates much of this burden by providing a fully managed service where the provider handles updates, security and maintenance. Hybrid-cloud solutions can combine elements of both, allowing businesses to customize their level of control.

**Cybersecurity prioritization.** Whether you choose an on-prem or cloud solution, ensuring strong cybersecurity practices is imperative. Choose a provider that prioritizes security from the start, not as an afterthought. Every deployment type should include encryption, network segmentation, and proactive security monitoring.

**Scalability and flexibility.** Considering the scalability of the system is key. Some access control providers require proprietary hardware that locks customers within their ecosystem. Selecting an open architecture solution gives you much more flexibility to gradually upgrade your hardware and software as your business changes, without the expense of having to rip out and replace legacy systems.

Businesses should carefully evaluate whether their chosen provider allows for open integrations and data portability. Even if a system supports existing hardware, some cloud providers limit interoperability through restricted APIs, proprietary data formats, or costly migration fees, making it difficult to switch providers in the future. 📧

*Kris Houle is a product line manager, Security Center SaaS, at Genetec Inc.*





# DOOR OPERATOR PRESENCE SENSORS

Detects Objects  
and Prevents Closure



## Guarantees Smooth and Safe Door Operation

SDC's **AUTO-IR** accessory mitigates injury liability and costly damage by detecting stationary objects and slow-moving people in the **swing path of an automatic door**. It's designed as a reliable companion accessory for virtually any door operator traffic application to **override ADA hold open time** and protect operator investment.

AUTO-IR **allows re-activation of the door** before contact is made during the closing

cycle, protecting slow-moving people as well as people trailing behind. It reliably detects stationary as well as moving objects in the swing path of an automatic door. **Following a door activation**, the AUTO-IR **remains enabled** to allow **continued automatic non-contact re-activation capability** should someone remain in the door opening while the door is open or while it is closing.

### AUTO-IR SERIES Presence Sensors



- 36" and 48" lengths
- Proven active infrared technology

### AUTO SERIES Low Energy Swing Door Operators



- Single button, self-tuning setup
- Built-in 1amp+ power supply
- Onboard lock sequencing

### 480 SERIES Narrow, Square & Round Push Plates



- Entire surface activates switch
- SPDT or DPDT
- Wireless or hardwired



*the lock behind the system*

sdccsecurity.com ■ 800.413.8783

[www.sdcsec.com/AUTO-IR](http://www.sdcsec.com/AUTO-IR)



# The Cybersecurity Time Bomb

By Will Knehr

If you work in physical security, you have probably seen it: a camera, access control system, or intrusion detection device installed years ago, humming along without a single update. It is a common scenario that security professionals have come to accept as “normal.” But here is the reality: this mindset is actively putting organizations at risk.

The security industry, manufacturers, integrators and end customers have a massive problem treating security technology like static infrastructure. Unlike a door or a fence, security devices today are essentially networked computers and leaving them untouched for years is no different than running an old Windows XP box on the open internet, a hacker’s dream.

## THE “INSTALL IT AND FORGET IT” MENTALITY

Most security deployments follow a familiar cycle:

**Step 1.** The sale is made. The customer chooses a security system based on features, cost, and brand reputation. Cybersecurity isn’t usually a significant factor in the buying decision.

**Step 2.** The system is installed. Integrators deploy cameras, access control, and other devices, get them up and running, and hand everything over to the end user.

**Step 3.** Nothing happens. No one thinks about firmware updates. No one checks for vulnerabilities. The system runs for years.

And then, one day, something happens. Maybe an attacker exploits an old vulnerability. Ransomware may lock down the entire network. Maybe an IP camera gets hijacked and used in a botnet attack. And suddenly, everyone is asking: “Why wasn’t this system secured?” The answer? Because no one took ownership of keeping it secure.

## WE SHOULD HAVE LEARNED BY NOW

A perfect example of this problem is Mirai, the botnet that weaponized thousands of unpatched IoT devices to launch history’s most significant DDoS attacks. When Mirai hit the news in 2016, it wasn’t exploiting some sophisticated zero-day (a software flaw that is unknown to the vendor or developers, meaning there is no patch or fix available).

The vulnerability had been patched years earlier. The problem was that most devices had never been updated.

Fast forward to today, and the same issue persists. Thousands of security cameras, NVRs, and access control systems are still unpatched on networks because no one prioritized updates. If Mirai wasn’t enough of a wake-up call, what would be?

## A THREE-WAY BLAME GAME

The problem is not just on one side. It is a perfect storm of bad habits from manufacturers, integrators, and end customers.

For their part, some manufacturers still design products with a ship-it-and-forget-it mentality. They build hardware, ship it and move on to the next model. Many devices still ship with default ad-

min passwords that never get changed. Firmware updates are often buried on a website somewhere with no automated update process.

Worse, some manufacturers treat their products as obsolete within a few years, even if customers still use them. This leaves integrators and customers on their own to secure products never built with cybersecurity in mind.

Integrators are stuck in the middle, expected to be cybersecurity experts whether they want to be or not. If a vulnerability is discovered after deployment, customers often turn to the integrator first, even if the manufacturer has not provided an update or the system is beyond its supported lifecycle.

However, integrators are running a business, and patching is not a revenue-generating activity. Customers are reluctant to pay for ongoing cybersecurity maintenance, and many integrators do not have a built-in service model for regular updates. Making matters worse, many security devices do not have easy remote update mechanisms. If firmware updates require on-site visits or manual downloads, they often do not happen.

End customers, meanwhile, often do not think about cybersecurity until something goes wrong. IT and security teams do not always communicate, leading to security devices connected to the main corporate network without proper segmentation, running on outdated firmware, and still using default passwords years after installation. Many customers assume their security devices are secure out of the box, but that is rarely true.

## BREAKING THE CYCLE

Fixing this problem starts with recognizing that cybersecurity is not a one-time setting; it is an ongoing process. Manufacturers need to take responsibility for long-term security by supporting products for longer lifecycles and shipping products with cybersecurity features enabled.

Integrators need to shift their approach as well. Cybersecurity can no longer be an afterthought; it needs to be built into service contracts with ongoing maintenance plans that include regular firmware updates and security checks. Security technicians also need better training on cybersecurity best practices, so they are not just installing equipment but actively securing it. Instead of leaving security configurations up to the customer, integrators should ensure devices are adequately secured at installation.

End customers must stop assuming cybersecurity is someone else’s job and start demanding more transparency from manufacturers. If a vendor cannot tell you how they handle security updates, that’s a red flag. Security devices should also be segmented from the leading network to prevent a single compromised device from exposing an entire organization. 🛡️

*Will Knehr is the senior manager of Information Security and Data Privacy at i-PRO Americas.*





# Control iD

## iDFace Max and iDFace

*Facial Identification Access Controllers*



### Facial Identification

Two 1080p Full HD cameras  
(visible light and infrared light)



### Number of Faces

Capacity for up to 100,000\*  
faces with live face detection



### LCD Touchscreen

7" touchscreen display  
and 3,5" touchscreen display



### SIP Intercom

Built-in G711 compatible  
SIP intercom\*



### Access Rules

Access rules according to  
schedules and departments



### Ingress Protection Rating

IP65 ideal for outdoor  
and indoor environments



### Connectivity

TCP/IP and USB

\*Available on select models



Learn more about  
iDFace Max and iDFace  
[controlid.com.br/en](http://controlid.com.br/en)

## ASSA ABLOY

# Paving the Way to Smart Buildings

By Emma Falck

In today's rapidly evolving security landscape, the convergence of on-prem, edge and cloud technologies are critical.

The physical security landscape is undergoing a profound transformation, driven by the rapid digitalization of buildings and the evolving needs of modern organizations. As the buildings sector pivots towards smart, AI and data-driven operations, the integration of both edge and cloud technology has become crucial.

Hybrid security solutions, which seamlessly blend traditional on-site systems with cloud-based capabilities, are emerging as an optimal approach to futureproof physical security for smart buildings.

## EMBRACING THE HYBRID ADVANTAGE

Hybrid security solutions combine the reliability and control of on-prem systems with the flexibility, scalability, and advanced capabilities of cloud architectures. This approach allows organizations to leverage their existing investments in physical security infrastructure while enhancing them with the benefits of cloud-based technology.

The hybrid approach can be considered a game-changer for the physical security market. The reasons are clear: It allows organizations to safeguard their security investments; enhance operational efficiency, availability, and resilience; and shift from capital expenditures (CAPEX) to operating expenses (OPEX).

Additionally, it unlocks new services such as false-alarm detection and remote maintenance diagnostics, facilitating a smooth transition to smart building capabilities. Key advantages of hybrid security solutions include:

**Protecting existing investments.** Hybrid solutions enable a gradual migration to cloud-based security, avoiding the need for costly and disruptive “rip and replace” overhauls of on-prem systems. Organizations can leverage their existing infrastructure while incrementally adding cloud-powered features and capabilities like mobile access, visitor management, and unified multi-site identity management.

**Enhancing maintenance and performance.** Cloud-based components of hybrid solutions offer enhanced maintenance, remote diagnostics, and automatic updates, resulting in a reduced workload for security teams. The cloud also enables improved data visualization, cross-domain use cases and harmonized resource management. Additionally, automation of tasks, as well as unified alarm and work management, allows for customization of workflows to streamline operations.

**Improving cybersecurity.** Hybrid architectures enable security managers to remotely monitor, diagnose, and update systems. By using edge hardware that allows for native cloud connectivity, robust protection against cyber threats is ensured. Cloud-based security services also provide the latest patches and cybersecurity features.

This is particularly important as new regulations like the EU

“By migrating from on-prem to cloud-based infrastructure, organizations can more easily connect access control and video data with building automation.”

Critical Entities Resilience Directive (CER) and the US Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) place increasing demands on organizations to strengthen their cybersecurity position. Therefore, security teams can comply with these new regulations more effectively by providing centralized visibility, remote management capabilities, and seamless integration of the latest security updates and protection.

**Increasing sustainability.** By migrating from on-prem to cloud-based infrastructure, organizations can more easily connect access control and video data with building automation, enabling occupancy-driven building management. This can reduce energy consumption by up to 65 percent.

## HYBRID SECURITY – THE HEART OF SMART BUILDINGS

Hybrid security is not just about physical protection – it is about unlocking the full potential of smart buildings. For example, access management systems can leverage occupancy data to improve visitor management, reduce food waste in canteens, and optimize smart heating and cooling.

Intelligent video management platforms, powered by cloud-based analytics, can differentiate between humans and animals, automate license plate recognition, and support real-time identity checks – all while ensuring compliance with local regulations.

Moreover, these solutions enable remote monitoring and management, allowing security teams to oversee multiple sites from a centralized cloud-based platform anywhere, anytime and from any device. This streamlines incident response, enhances overall safety and reduces the workload for operators.

Ultimately, by seamlessly blending on-prem and cloud technologies, organizations can protect their investments, enhance operational efficiency, improve cybersecurity, and drive sustainability. This lays the foundation for a new era of intelligent, user-centric buildings.

Hybrid security is not in the future – it is here now. Forward-thinking organizations are already embracing this approach to stay ahead of the curve and deliver the secure, smart and sustainable buildings of tomorrow. 📱

*Emma Falck is the executive vice president, Product, at Siemens Smart Infrastructure Buildings.*





# 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



## Quanergy Solutions, Inc.

Is showcasing its comprehensive portfolio of hardware and software solutions for both outdoor and indoor applications. Featured products include Q-Track 2.4 software with powerful AI-driven insights; Q-Track LR for long range intrusion detection and perimeter protection; Q-Track HD for optimal detection, tracking and classification in challenging environments like airport terminals, retail stores and office buildings; and Q-Track Dome to track and classify people in smaller and more complex environments, such as corridors, mantraps and line queues.



## AMG Systems

Introducing the AMG260B/AMG2036 Blade Chassis System. The AMG260B blade cards are designed for installation in the AMG2036 blade chassis system, which accommodates up to 18 individual blade cards within a single 1U of 19-inch rack space. This configuration offers industry-leading rack density, where space is limited, and the blade cards' hot-swap capability facilitates easy future expansion and device maintenance or replacement. Models are available with one TX port in, one FX SFP port out, and two TX ports in, one FX SFP port out, with additional models planned.



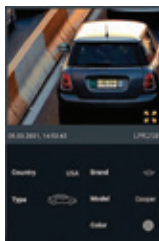
## Delta Scientific Corp.

Bollards are fixed barriers that restrict physical access to an area. They are used to limit vehicle traffic. Pedestrians can easily walk in the spaces between well-placed bollards, but cars cannot pass through. Examining key bollard statistics provides insight into how they improve safety. Bollards can help prevent up to 100 building crashes daily. The global bollard market is expected to reach \$4,512.9 million by 2032. Bollards are a proven solution for mitigating threats, protecting people and securing properties



## HANWHA Vision

An edge based LPR camera solution, Wisenet Road AI, uses AI camera technology to help identify vehicles on the road. These License Plate Recognition (LPR) cameras featuring Make, Model, and Color Recognition (MMCR) can accurately capture vehicle information in various traffic conditions ranging from low-speed parking situations to free-flowing highway scenarios. It also includes license plate recognition (LPR) with supporting images, efficient smart search, insight and statistics dashboard, and VMS Integration.



## Altronix Trove™ Series

Comprehensive pre-wired, pre-configured access and power kits supporting over 50 leading access control brands including AMAG, AXIS, Azure, Brivo, Hirsch, Mercury, Software House and TDSi. Easily combine Altronix power with access controllers in scalable wall-mount to extended rack-mount configurations for any installation environment, providing a single point for service and maintenance, minimizing wall space. The company's latest innovations, including integrated power and access control solutions that streamline installation and reduce labor costs, and the latest solutions to deploy IP devices using coax, fiber or Ethernet infrastructure.



## Marks USA

Newly released, Marks USA, a division of NAPCO Security Technologies, Inc., has announced the SKA-Series Indicator Locks. These locks offer a highly visible security status at a glance — perfect for schools, healthcare facilities, offices, and commercial buildings. The new Marks Indicator Locks are now available through Marks' locksmith and security dealer partners nationwide. Designed for today's heightened focus on safety, Marks' Indicator Locks feature bold red and green visual indicators.



## Rohde & Schwarz

A significant milestone has been reached receiving approval of detection capability from the European Civil Aviation Conference (ECAC) for its QPS Walk2000, making it the world's first walk-through millimeter wave security scanner allowed for use at airports. This certification underscores that the advanced scanner meets ECAC's rigorous aviation security detection requirements for screening on-person threats. Rohde & Schwarz is set to deploy these advanced scanners throughout the European Union, enhancing passenger screening at airports across the region to an unprecedented level.



## Zenitel

Has launched two new innovations for mixed-use building communication solutions: the Zenitel Display Door intercom (ZDD-1) and the Zenitel Slim Door intercom (ZSD-1). This further strengthens Zenitel's position in audio communication solutions. With 125 years of experience in sound design, these new door entry intercoms are engineered from the ground up, offering a premium audio experience in a sleek design that seamlessly blends into any building. Door entry intercoms are an essential part of overall building security.







### SAFR from RealNetworks

Attendees at ISC West were able to experience its revolutionary suite of AI-powered solutions. SAFR's facial recognition technology delivers unparalleled certainty through industry-leading accuracy, enabling organizations to monitor and analyze visual data at speeds far beyond human capabilities—all while maintaining the highest standards of data privacy and personal control. The Unified Facial Recognition Ecosystem represents a fundamental shift in how organizations manage access across their enterprise, bringing unparalleled efficiency, accuracy, and scalability through a single cohesive platform.



### Camden Door Controls

The launch of its new 1420 Series Low-Profile Fire-Rated Strike is designed to provide a cost-effective solution for code compliance in UL fire-rated doors and frames with cylindrical locksets. Built to the highest industry standards, the CX-ED1420 strikes are Grade 1 ANSI fire-rated and engineered for 1/2" to 5/8" latch projection. They offer exceptional durability with 1,500 lbs static strength and are factory-tested for an impressive 1.5 million cycles.



### AMAG Technology

Symmetry CompleteView Video Management 7.5, the latest software update to its video management system (VMS) platform. This version enhances operator experiences and introduces significant new enterprise capabilities including the integration of Iron Yun's Vaidio® AI Video Analytics. The integration of Vaidio® AI Video Analytics provides a comprehensive suite of advanced analytics for people, vehicles, facial recognition, and objects, compatible with any camera or video source. This enhanced solution supports both real-time monitoring and forensic investigations.



### Alarm Lock

Introducing its new TL-series Trilogy Touch™, Alarm Lock, a division of NAPCO Security Technologies Inc., says this is part of its class-leading standalone and wireless networked models. This aesthetic access control solution features a sleek and modern EZ Touch Sense Panel, with illuminated numbers that light up when touched and dim after use, in place of the standard all-metal keypad, for which Trilogy's are well known. The TL-Series still offers all the same functionality and operation, weather proofness, and minimal maintenance requirements for the lowest total cost of ownership.



### HID Global

As the industry accelerates its shift toward mobile-first and seamless security integrations, HID has been working on solutions to create smoother and more secure access across touchpoints—from entryways to internal systems—optimizing workflows and minimizing disruptions. HID is at the forefront of driving a world of seamless security, combining our deep expertise with continuous innovation to meet the evolving needs of modern access control and identification.



### Prodata Key

This enhancement of PDK.io has been shaped entirely by partner feedback and needs. Customers told PDK staff that PDK.io could be even easier with improved navigation and keeping key information in context. Not only does this update allow PDK.io to look and feel more modern, but it is also the fastest experience yet. The updated PDK.io uses a drawer-based in-context editing system, allowing users to maintain their workflows while staying in context.



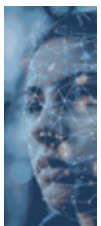
### AXIS Communications

The Q8752-E Mk II gives you two excellent cameras in one: a thermal camera for reliable detection and verification around-the-clock and in all weather and light conditions, and a visual camera for outstanding visual identification purposes. It offers a ground-to-sky view with a tilt range of -90° to +45° and 360° infinite pan for fast camera repositioning and smooth tracking of objects. Thermal palettes help identify different heat sources emitting the same amount of thermal energy, making it easier and more efficient to interpret a scene.



### MERON

Introducing an incident management solution MERON PIAM+ leverages the latest advancements in data science, AI and microservices architecture, setting new benchmarks in performance and cost efficiency for large enterprise applications. MERON PIAM+ integrates advanced AI technologies, automation and analytics to provide enhanced security, efficiency and adaptability. The solution employs the latest concepts in computer science including in-memory data structures, infinitely scalable microservices, data management architecture, streaming data analytics and integration and an advanced AI engine that drives intelligent Co-pilots to automate tasks and workloads.



## Schlage

Electromechanical locks are a versatile Electronic Access Control (EAC) solution that can be managed locally by a card reader or actuator and controller or a simple remote release switch. They offer a dependable, wired solution as part of a facility-wide EAC integration. Schlage electrified locks can be configured for multiple functions and a wide selection of finishes and designs in mortise, mortise multi-point and cylindrical locks.



## Dotworkz

In the world of surveillance, Power over Ethernet (PoE) plays a crucial role in ensuring a seamless and efficient power and data connection for security cameras. Dotworkz, a leader in innovative camera housing solutions, primarily used Pass-Through PoE in its housings to accommodate various installation needs. We explore the key differences between Passive PoE and Pass-Through PoE in Dotworkz camera housings and how they impact your surveillance setup.



## Platinum Tools

The Standalone Fiber Scope is compatible with Android & iOS for seamless viewing and reporting, provides zone testing and reporting, includes adapters for 2.5mm and 1.25mm connectors, and works with Platinum Tools, PT-OTDR-100 for quick, detailed results. The new CCTV Tester allows for the powering and viewing of PoE cameras, provides Wi-Fi camera access, has RJ45 continuity testing and TDR length measurement, and its network tests include IP scan, ping DHCP and trace route.



## AtlasIED

The launch of the new Rapid Alert system includes the IP-PB wearable panic button and the IP-RC BLE-controlled relay board. This system is designed to enhance emergency communication and integrates seamlessly with AtlasIED's IPX IP Endpoints, providing immediate accessibility to trigger notifications during critical events. The IP-PB panic button is worn on a lanyard and connects wirelessly to the IP-RC relay board via Bluetooth Low Energy. Users can press the panic button to activate notifications, including pre-programmed alerts that play throughout the facility.



## Zentra

A simple connection point for your multi-family building needs. Whether you are an integrator, owner or property manager we are here to meet your needs. With Zentra, property owners and managers can run properties efficiently and provide their residents with seamless and trusted security. Zentra ties all access points of your property together in one system, saving time, money and hassle.



## Intellicene

Announcing a unified security management, Intellicene's Monitoring Hub, a solution designed to simplify and automate security system health checks has hit the market. By continuously monitoring the status of devices across a network, including cameras, servers and edge devices, it ensures the system's health while also offering clear insights to address any issues before they disrupt operations. Security teams face increasing pressure to manage large-scale, multi-site security systems efficiently. Manual monitoring methods are time-consuming and prone to inaccuracies, often resulting in vulnerabilities and operational downtime.



## Robotic Assistance Devices

RIO Mini has launched as a compact, solar powered, AI-backed mobile surveillance trailer. It was previewed and received strong attention from industry insiders, end-users and dealers. It delivers core RAD capabilities, including Autonomous Intelligent Response, at a lower cost of entry and it is expected to be RAD's most profitable product line yet, forecasted to add up to 500 units this fiscal year. It runs a dual ROSA configuration and is powered by RAD's award-winning SARA platform.



## Von Duprin

Outdoor Defense products are designed to perform in outdoor applications such as courtyards, perimeter security, rooftops, and patios and are engineered to safeguard against moisture, temperature variations, and corrosion in normal outdoor conditions. Available for the popular 98/99 series push pad, this option offers advanced protection to components enabling the device to function in external environments.





Company Name	Page	Company Name	Page	Company Name	Page
<b>ADVERTISERS</b>					
Altronix.....	5	AMG Systems.....	30	Meron.....	31
ASSA ABLOY DSS.....	27	AMAG Technology.....	31	Platinum Tools.....	32
ASSA ABLOY EMS.....	17	AtlasIED.....	32	Prodata Key.....	31
Axis Communications, Inc.....	36	Axis Communications.....	31	Quanergy Solutions Inc.....	30
Camden Door Controls.....	3	Camden Door Controls.....	31	Robotic Assistance Devices.....	32
CyberLock, Inc.....	23	Delta Scientific Corp.....	30	Rohde & Schwarz.....	30
Door King.....	21	Dotworks.....	32	SAFR from RealNetworks.....	31
MIER PRODUCTS, INC.....	7	Hanwha Vision.....	30	Schlage.....	32
MIER PRODUCTS, INC.....	19	HID Global.....	31	Von Duprin.....	32
Napco Access Pro.....	35	Intelllicene.....	32	Zenitel.....	32
Robotic Assistance Devices.....	13	Marks USA.....	30	Zentra.....	32
ROLLOK Rolling Doors and Security Shutters.....	11				
Security Data Supply.....	2				
Security Door Controls.....	25				
Traka USA.....	9				
Viking Electronics.....	29				
<b>Security Today Solutions</b>					
Alarm Lock.....	31				
Altronix Trove.....	30				

## A Closer Look at Verkada

EPISODE 35

SPONSORED BY

**Jake Leichtling**  
Director of Product Management for  
Access Control at Verkada

# A Model for Community Security

By Nick Smith

**T**he Community Builders (TCB) is a nonprofit organization whose mission is to build and sustain strong communities where all people can thrive. They work with businesses, institutions and public officials to revitalize neighborhoods in ways where all people can live in healthy homes with equitable access to resources and opportunities to pursue their dreams.

Their partnership with Salient Systems exemplifies the use of video technology in vulnerable neighborhoods to help achieve these goals. TCB operates and manages 150 sites and properties across the country, employing over 600 staff members.

## VULNERABLE NEIGHBORHOODS

These locations range from campus environments to individual buildings, each presenting unique security challenges to ensure overall resident safety. The primary focus for implementing a video management system is not only to ensure safety and security but also prevent property maintenance issues.

Under Joe Giggey's leadership as senior director of Information Technology, TCB established enterprise level security standards. These standards enabled access to video remotely through smartphones, iPads, and laptops for a central team of sites in 30 cities.

Additionally, seamless integration with existing cameras and access control systems was required, considering TCB's extensive network of 30+ access control systems and about 6,800 different camera models.

Affordability was another crucial factor, as is often the case for nonprofit organizations. Having an easy-to-administer VMS, reliable search and video export functionalities, scalability for future property acquisitions, and centralized management in a distributed environment were also significant requirements.

Salient's CompleteView VMS met all the specified criteria, marking the beginning of the partnership between TCB and Salient



DC Studio/stock.adobe.com

in 2016. The deployment of CompleteView has grown to 85 site recording servers and more than 2,300 camera licenses.

## CERTIFIED INTEGRATORS

Given the widespread nature of TCB's properties, certified regionalized integrators have been selected to install CompleteView across TCB locations. These integrators have been trained and received certification from Salient Systems professional trainers on installation, executing upgrades, expanding systems, and customizing the deployment ensuring effective implementation and ongoing support.

In addition, manufacturer support by the Salient system engineering team has been used and according to TCB staff, "has been phenomenal." TCB staff help address complaints, educate residents on lease rules, and avoid evictions. The software has assisted in resolving disputes and investigating incidents.

In addition, the ability to verify details of incidents in progress helps pinpoint the

location and gives first responders details about the situation they may face on arrival. Video footage provided by Salient's VMS has proven invaluable in multiple instances and according to Giggey "The VMS paid for itself immediately, highlighting the effectiveness and value of this partnership."

The collaboration between TCB and Salient Systems has become an exemplar of how technology can be harnessed for the greater good, building trust and effecting positive changes in vulnerable neighborhoods. With ongoing support, TCB is committed to making a lasting impact and ensuring strong communities where all people can thrive. 📺

*Nick Smith serves as vice president of Sales for Salient Systems, where he leads sales strategy and team performance across the Eastern United States.*





# Turn Every Door into Recurring Revenue



**With Napco's MVP Access & EZ Cloud Platforms—  
*One for Scale, One for Simplicity***



## **Choice of 2 Affordable, Scalable *By-Door* Access Systems Designed for Integrators, Dealers & Locksmiths:**

- Up & Running in a Few Quick EZ Steps to New RMR
- No on-premises PC or database required.  
*With MVP EZ there's No Computer Required!*
- Native Integration with Alarm Lock Trilogy® Networx & ArchiTech Locks
- Integrated with new NA-Series & new or existing Continental Access Panels
- Provide Lockdown & SMS Text & Email Alerts for Users' Safety
- Easy MVP EZ App - Control, Configure & Command System Solely Using a Smartphone - Add Doors/Devices by scanning them with the camera
- **OR** Enterprise MVP Access App—Mobile credentials w/geo-fencing, MFA & remote admin functions, e.g., lock or open doors from anywhere



Contact us for more or an intro demo  
call 1.800.645.9445 | [www.napcosecurity.com](http://www.napcosecurity.com)

Get  
Started





# Multi-layered protection at every stage.

Mitigate cybersecurity risks throughout the device lifecycle.

Protecting your network devices from cyberthreats is vital throughout the entire device lifecycle. A 'set-and-forget' approach towards implementing new technology can leave your system vulnerable to emerging threats and exploits. Axis device management software gives you the centralized control and insight you need to apply safeguards, maintain compliance and ensure software is always up-to-date so your devices receive all the latest bug fixes and vulnerability patches.



Read more:  
[www.axis.com/products/device-management-software](https://www.axis.com/products/device-management-software)

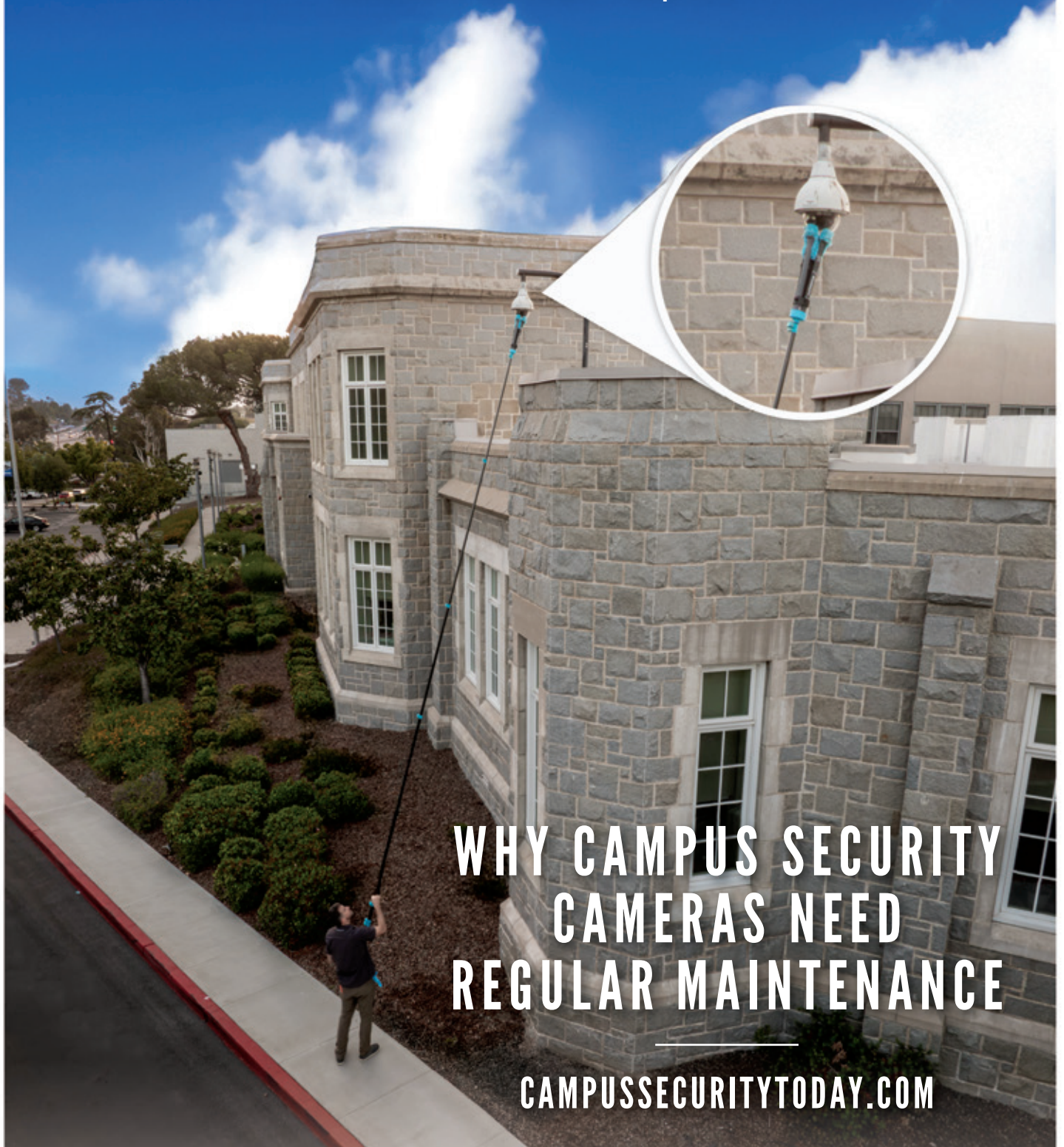
**AXIS**<sup>®</sup>  
COMMUNICATIONS



MAY/JUNE 2025

# CAMPUS SECURITY TODAY

education | healthcare | corporate



WHY CAMPUS SECURITY  
CAMERAS NEED  
REGULAR MAINTENANCE

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





# Sometimes our **biggest priorities** come from the smallest of reasons.

Keeping our kids safe and secure in schools starts with a decision to prioritize it. The next step? PASS and Axis.

The Partnership Alliance for Safer Schools (PASS) is a non-profit, unbiased resource for non-security experts. For over 10 years, PASS has brought together safety and security experts from across the industry to research and evaluate best practices, and to develop actionable, constantly updated guidelines to help you keep your school safe and secure.

Thanks to the ecosystem of all PASS partners – like Axis Communications – these guidelines are available for free.

With PASS and Axis, you can turn your priorities into actions. For all the small reasons.



Download the guidelines





It takes a Viking to...

# PROTECT WHAT MATTERS



**KEEP YOUR CAMPUS  
SAFE & SECURE**

When it comes to the safety of your students, we **won't compromise**. You need solutions that are both strong and dependable.

Viking Entry Systems and Emergency Phones are designed for **long-lasting performance**, with optional Enhanced Weather Protection providing extra defense in tough outdoor conditions.

Say goodbye to unreliability, and hello to rugged durability... **YOU NEED A VIKING.**



# VIKING

715.386.8861

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



DESIGNED  
MANUFACTURED  
& SUPPORTED



# CONTENTS

## 06 CAMPUS VIEWPOINT

### 08 LET'S BE CLEAR: WHY CAMPUS SECURITY CAMERAS NEED REGULAR MAINTENANCE

### 12 USING EMERGING TECHNOLOGIES TO ADDRESS HEALTHCARE STAFFING, WORKPLACE VIOLENCE ISSUES

### 16 HOW TO HARNESS ALPR FOR GREATER SECURITY, EFFICIENCY AND COLLABORATION

### 18 HOW EMERGING TECHNOLOGIES ARE TRANSFORMING THE SCHOOL SECURITY LANDSCAPE

### 20 SECURING HIGHER EDUCATION: COMBATING ENROLLMENT FRAUD AND EMPOWERING STUDENT FINANCIAL SUCCESS

### 22 HOW COMPOSABLE SECURITY TECHNOLOGIES FORTIFY CAMPUS SAFETY

# AD INDEX

ASSA ABLOY DSS	5
ASSA ABLOY EMS	13
Axis Communications, Inc.	2
Campus Security Today Webinar	19
CEIA USA	9
Dotworkz	23
Napco Access Pro	24
Overly Door Company	11
Paxton Access, Inc.	15
Traka USA	7
Uline	17
Viking Electronics	3



WHY CAMPUS SECURITY CAMERAS  
NEED REGULAR MAINTENANCE

COVER PHOTO:  
COURTESY OF DOTWORKZ

# Creating access for the future



With an approach that balances safety, security and wellness, you can create an atmosphere that provides peace of mind for students, faculty and staff.



**Door status indicators** provide quick and easy confirmation whether a door is locked.



**Access control** enables application-specific lockdown strategies throughout schools.



**Attack-resistant door openings** keep occupants safe and secure and delay intruders from entering.



**Red button locking solutions** empower anyone in the classroom to lock it down instantly.



Helping schools create a safe and secure learning environment is a top priority for ASSA ABLOY. We are here to help you evaluate your safety and security needs and assist with any questions or concerns you may have.

Learn more at [assaabloydss.com/k12](https://assaabloydss.com/k12)

**ASSA ABLOY**  
Opening Solutions

Experience a safer  
and more open world

# HOW REALISTIC SHOULD ACTIVE SHOOTER DRILLS BE?

BY BRENT DIRKS

MAY/JUNE 2025

A major part of school security is preparedness for the unthinkable. Active shooter drills are one way to prepare students, teachers, and administrators for an event.

But law enforcement and school districts continue to struggle with the question of how realistic should these drills be. In early April, at Snowflake High School in Snowflake, Arizona, the school conducted an unannounced drill.

According to local news station 12News, instead of bell for a drill, a “more serious” bell rang.

School District Superintendent Hollis Merrell described the bell to the station:

“It audibly says, ‘This is not a drill,’ but it doesn’t give any indication as to what may be happening at the school. It’s just locked down. This is not a drill. The police are on their way,” Merrell said.

The Taylor-Snowflake Police Department approached the school to make the active shooter drill more realistic. It was designed to mimic a real emergency situation.

Because of the approach, students, some staff, and parents were unaware of the drill. Some students assumed the worse and texted parents that there was an active shooter on campus.

Police Chief Robert Martin said the unannounced drill idea came after a previous drill in late 2024 where he felt students were not taking the drill seriously.

Obviously, students should take every drill seriously. But that sometimes doesn’t happen. High schoolers can simply be high schoolers and not understand how important drills are to prepare the school community.

I understand Chief Martin’s frustrations, but the unannounced drill likely took the situation too far.

Communication and trust between everyone are undeniably important parts of school security at any level. While students at Snowflake High School will likely start taking drills more seriously, why dent those bonds between the school, community at large, and law enforcement? There are better ways to make the point. ♥



*Brent Dirks*

Brent Dirks  
bdirks@1105media.com

## **CAMPUS SECURITY TODAY TEAM**

PUBLISHER: ralph c. jensen; EDITOR: brent dirks; SENIOR ART DIRECTOR: laurie layman; PRINT MEDIA TECHNICIAN: joanne kim; INTEGRATED MEDIA CONSULTANT-U.S.: brian rendine, 972.687.6761; INTEGRATED MEDIA CONSULTANT-U.K. & EUROPE: sam baird, +44 1883 715 697

## **INFRASTRUCTURE SOLUTIONS GROUP**

PRESIDENT: dan labianca; PUBLISHER/EDITOR IN CHIEF: ralph c. jensen; CIRCULATION DIRECTOR: tillie carlin; WEBINAR ADMINISTRATOR: tammy renne

## **1105 MEDIA, INC. EXECUTIVE TEAM**

CHIEF EXECUTIVE OFFICE: rajeev kapur; CHIEF FINANCIAL OFFICER: sanjay tanwani; CHIEF TECHNOLOGY OFFICER: eric a. lindgren; EXECUTIVE VICE PRESIDENT: michael j. valenti;

## **CONNECT WITH US**

EDITORS AND CONTACT INFORMATION: available at [www.campussecuritytoday.com](http://www.campussecuritytoday.com); CORPORATE OFFICE: m-f, 8:30 a.m. – 5:30 p.m. pt, 818.814.5200, 6300 canoga avenue, suite 1150, woodland hills, ca 91367





## Campus-wide security always within reach

Traka Touch Pro key cabinets help decentralize physical keys across your campus, with total control and visibility of all activity

**traka**  
ASSA ABLOY

Visit [traka.com](https://traka.com) to explore your path to a safer and more secure campus





# LET'S BE CLEAR: WHY CAMPUS SECURITY CAMERAS NEED REGULAR MAINTENANCE

AUTHOR: WILLIAM FERRIS IS CEO OF DOTWORKZ.  
IMAGE: COURTESY OF DOTWORKZ



“

REGULAR MAINTENANCE ENSURES SURVEILLANCE SYSTEMS CAPTURE CLEAR, USABLE FOOTAGE, REDUCE FALSE ALARMS, EXTEND THE LIFESPAN OF SECURITY EQUIPMENT, AND LOWER LEGAL AND INSURANCE RISKS.



# GAME DAY AT RECORD SPEED.



## **OPENGATE®** *Groundbreaking Weapons Detection System*

- Quickly and automatically screen guests with their backpacks, purses and bags in transit
- Extremely high throughput with near zero nuisance alarms
- Detects handguns and mass casualty threats, such as high caliber assault weapons and IEDs
- Easy to relocate at 25 pounds and installs in less than 1 minute
- Indoor and Outdoor operations

Our Weapons Detection and screening systems take the guesswork out of security screening. Incorporating the latest in threat detection technology, CEIA (CHAY-ah) sets the standard for safety, convenience and accuracy.

For more information, contact your CEIA USA representative at [security@ceia-usa.com](mailto:security@ceia-usa.com) or call us today at 833-224-2342.





Universities invest in security camera systems, expecting them to provide clear, reliable footage to help protect students, faculty, and staff. These cameras are strategically placed across campus—monitoring entryways, dormitories, parking lots, stadiums, bookstores, and common areas—as both a deterrent to crime and a valuable tool in incident investigations.

However, security cameras are often left to collect dust, pollen, webs, and debris. Even the most advanced security cameras cannot function effectively if their lenses are covered in residue. High-definition, infrared, or license plate recognition cameras become useless if they can't see clearly. Over time, dirt, water spots, and environmental debris accumulate, degrading image quality and creating security blind spots. Unfortunately, camera cleaning and maintenance are often overlooked on college campuses, leading to security failures, increased liability risks, and unnecessary costs.

#### THE ROLE OF IT AND FACILITIES IN CAMERA MAINTENANCE

At most universities, security cameras are the responsibility of multiple departments. The IT team ensures the cameras are integrated with the network, configured properly, and store footage efficiently. Facilities teams manage the physical upkeep, ensuring the cameras are mounted securely, protected from the elements, and operational in all conditions. Campus security relies on these cameras to monitor live activity, respond to threats, and review footage when incidents occur.

Despite this shared responsibility, routine cleaning often falls into a gray area, with no department taking ownership. Cameras in high-traffic areas—such as parking lots, walkways, stadiums, bookstores, and dormitory entrances—quickly accumulate dust and debris. License plate recognition cameras used for parking enforcement are particularly vulnerable to pollution and residue buildup, which can obscure plate numbers and lead to citation errors.

Building-mounted cameras, often installed on rooftops for an elevated security view, face unique challenges. These cameras are constantly exposed to the elements, including wind-blown debris, bird droppings, and extreme weather conditions. Without routine cleaning, rooftop security cameras lose their effectiveness, creating blind spots that compromise campus safety.

#### THE COST OF POOR CAMERA MAINTENANCE

Neglecting security camera maintenance can lead to both financial and legal consequences. If an incident occurs and the available footage is too blurry to be useful, the university may face lawsuits, insurance disputes, and public criticism for failing to maintain proper security.

Beyond legal exposure, poor maintenance also leads to unnecessary equipment failures. Cameras that are not cleaned regularly are more likely to experience lens scratches, internal water damage, and overheating due to dust-clogged ventilation. These issues shorten the lifespan of the cameras, forcing universities to replace equipment more frequently.

Given the investment universities make in security technology, allowing cameras to deteriorate simply because they are not cleaned is a preventable waste of resources. A simple, scheduled maintenance plan can extend the life of security cameras, ensuring they function effectively for years rather than requiring premature replacements.

#### THE IMPACT ON SECURITY OPERATIONS

Campus security officers and emergency response teams rely heavily on camera footage to assess situations in real time and investigate past incidents. If a camera is dirty, its field of view may be obstructed, limiting the ability to detect threats or identify individuals.

Night vision and infrared performance are particularly affected by dirty lenses. Many security cameras use infrared technology to capture images in low-light conditions, but dust and smudges on the lens scatter IR light, creating glare that can make footage unusable.

False alarms are another issue caused by unmaintained cameras. Many modern security cameras use motion detection technology to trigger alerts, but when cameras are covered in spider webs or dust, they can mistake small debris movements for suspicious activity. This results in wasted security resources as officers investigate non-existent threats instead of focusing on actual security risks.

Bookstores and campus retail locations also rely on security cameras for loss prevention. A camera monitoring transactions and store aisles is only as effective as the visibility it provides. If the footage is obstructed or blurry due to dust or webs, incidents of theft, fraud, or misconduct may go undetected, impacting the university's revenue and asset protection efforts.

By keeping cameras clean, security teams reduce false alarms, improve nighttime surveillance, and ensure officers have access to reliable video evidence when they need it most.

#### THE POWER OF INNOVATION

Traditional cleaning methods, such as wipers or paper towels, can leave streaks, cause static buildup, or even scratch the delicate lenses of security cameras. The most cost-effective method for cleaning cameras is using shape-shifting microfiber cleaning head tools, which outperform standard wipers without damaging lenses or requiring fluid refills.

Microfiber cleaning heads not only remove pollution and salts but also polish the lens surface, improving clarity and reducing light distortion. New materials now have anti-static properties that prevent dust and pollen from immediately resettling on the lens, ensuring cameras stay clean for a longer period.

Unlike basic cloths or wipers that simply push debris around, microfiber mitts trap and lift dirt without damaging sensitive optics. This is especially important for high-end security camera lenses that require pristine clarity for advanced analytics and image processing.

#### ELIMINATING LADDERS AND LIFTS FOR SAFER CLEANING

Another often overlooked factor in camera maintenance is workplace

safety. Many security cameras are mounted on high poles, rooftops, or building exteriors, requiring ladders or aerial lifts for cleaning.

From an occupational safety standpoint, sending workers up a ladder in a high-traffic area presents serious fall risks. Students and staff walking nearby may accidentally bump into the ladder, increasing the chance of an accident. OSHA guidelines discourage unnecessary ladder use in public spaces, and university insurance carriers recognize the risks associated with fall hazards.

To eliminate these risks, the Dotworkz DomeWizard security camera cleaning kits allow maintenance staff to clean cameras from the ground. New extendable cleaning tools range from 13 feet, 25 feet, and 40 feet, plus the operator's height, making them capable of reaching even the highest-mounted cameras without requiring a lift.

By switching to ground-based cleaning methods, universities can reduce workplace injuries, avoid OSHA compliance issues, and improve overall efficiency in security camera maintenance.

#### A NEW REVENUE OPPORTUNITY FOR CAMPUS SERVICE PROVIDERS

With the introduction of modern camera service tools, camera maintenance is now a job that can be performed quickly, safely, and professionally. For professional campus service providers, this presents a new revenue opportunity. Camera maintenance, which previously required costly lifts and multiple personnel, can now

be completed in just minutes with extendable cleaning systems.

A single cleaning service can pay for the cost of the tools, making it a worthwhile investment for service providers looking to expand their offerings. Security and facilities teams that previously avoided camera maintenance due to safety concerns can now easily incorporate it into their regular service schedule. With minimal training, maintenance staff can ensure cameras remain clean year-round, reducing downtime and improving surveillance quality.

#### THE LONG-TERM BENEFITS OF ROUTINE CAMERA MAINTENANCE

Cleaning security cameras is one of the simplest and most cost-effective ways to improve campus security. Regular maintenance ensures surveillance systems capture clear, usable footage, reduce false alarms, extend the lifespan of security equipment, and lower legal and insurance risks.

For universities, the message is clear—security technology is only as effective as its upkeep. By making camera maintenance a standard practice and using microfiber cleaning heads for superior performance, campuses can maximize their investment in surveillance systems while ensuring a safer environment for students, faculty, and staff. ♥



## Overly: The First Name—And The Last Word—In Specialty Doors.

Acoustic Doors		Bullet-Resistant Doors	
Metal	Wood Finish	Metal	Wood Finished
<ul style="list-style-type: none"> <li>• Metal Swinging Doors</li> <li>• Fixed Window Systems</li> <li>• STC ratings from 43 to 57</li> <li>• Available with up to 3-hour fire labels</li> </ul>	<ul style="list-style-type: none"> <li>• STC ratings of 43 to 50</li> <li>• Dual-glazed Vision Lights</li> <li>• Wood veneers and plastic laminates</li> <li>• 3/4 hour and 20 minute fire labels</li> </ul>	<ul style="list-style-type: none"> <li>• Weapon Protection Levels 1-8</li> <li>• UL Standard for Safety 752</li> <li>• Fixed and Teller Window Systems</li> <li>• Pass-Throughs, Gun and Voice Ports</li> </ul>	<ul style="list-style-type: none"> <li>• UL Standard for Safety 752</li> <li>• Weapon Protection Levels 1-8</li> <li>• Single or pair configurations</li> <li>• Wood veneers and plastic laminates</li> </ul>

**OVERLY**  
DOOR COMPANY

overly@overly.com • www.overly.com





# USING EMERGING TECHNOLOGIES TO ADDRESS HEALTHCARE STAFFING, WORKPLACE VIOLENCE ISSUES

AUTHOR: MATT KJIN IS SEGMENT DEVELOPMENT MANAGER – HEALTHCARE AT AXIS COMMUNICATIONS.

IMAGE: GREENBUTTERFLY/STOCK.ADOBE.COM

**T**he healthcare industry consistently adopts new technology to address challenges across all of its sectors. Many of the emerging technologies that are available today are being applied to optimize workflow. To enhance their operational efficiency, hospitals and other healthcare providers typically embrace emergent technologies to streamline tasks in patient care, administration, and, of course, security.

Underlying the need for better operational efficiency is a troubling reality: hospitals face significant challenges today, including a shortage of staff and behavior-related issues that can escalate into violence. For instance, healthcare workers are four times more likely to experience serious workplace violence, according to the American Hospital Association. A report published last year by National Nurses United reveals that eight in 10 nurses had experienced at least one type of workplace violence during the prior year.

The healthcare system faced staff shortages well before the pandemic and they continue to grow. Research from the National

Council of State Boards of Nursing discovered that around 100,000 registered nurses (RNs) left the workforce during the COVID-19 pandemic, citing stress, burn-out or retirement. Even more alarming is the fact that 800,000 additional RNs have expressed their intention to leave the workforce by 2027 for similar reasons.



Understaffing in the healthcare industry has been widely studied, and technology stands out as a good solution for certain workflows. Emerging tools seamlessly integrate into the workflows that make up this human-centered environment. These tools provide data that enhance efficiency and allow staff to focus more on patient care, including monitoring high-risk situations to keep them from escalating. Interestingly, while some industries focus on gathering business intelligence and gain operational efficiencies as a byproduct, that is reversed in the clinical world. Focusing on operational efficiencies in healthcare often produces business intelligence data as byproduct, which hospital administrators then can use to make data-driven decisions.

Almost every healthcare facility in the U.S. uses some form of video. The applications for it include security and safety, remote patient monitoring, virtual nursing, administrative tasks, and even monitoring situations such as occupancy levels and suspected medication diversion.

There are clear guidelines associated with where and how healthcare organizations can implement video technology, so that they meet the requirements of the Health Insurance Portability and Accountability Act (HIPAA). The American Hospital Association explains what to consider from a compliance perspective. According to a January 2025 article in *The HIPAA Journal*, since Protected Health Information (PHI) cannot be separated from other data recorded by surveillance cameras, all footage (when recordings are used) must be secured in



ASSA ABLOY

Advanced  
Monitoring  
Options

Retrofit-Ready  
Designs



Preload  
Capable  
Designs

Third-Party  
Certified  
Strength &  
Durability

Simplified  
Installation  
Templates

Flexible  
Mounting &  
Adjustment

Complete  
Pac: One  
Box Solution

Architectural  
Finish Options

Modular  
Faceplates  
& Mounting  
Hardware



Widest  
Range of  
Applications

# More Features. More Options. More Possibilities.

## Designed to Do More, So You Can Too.

We don't just meet industry standards—we exceed them.

**Our features give you more options**, delivering the flexibility to secure any opening. Choose from **advanced monitoring**, **durable finishes**, **preload solutions**, and **third-party certification testing** to ensure reliability where it matters most. When you need more from your access control, **we deliver possibilities.**

*Every Lockset. Every Application.*

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

Experience a safer  
and more open world



compliance with the safeguards outlined in the HIPAA Security Rule.

### WEARABLE CAMERAS

One form of video—wearable cameras—is becoming a sought-after emerging technology to act as a behavioral modifier or record escalating behavior. These devices also are ideal for documentation in general.

The International Association for Healthcare Security and Safety (IAHSS) Foundation offers a comprehensive overview of the regulatory and legal considerations, titled “Body-Worn Cameras in Healthcare.” This guide is like a decoder ring for a hospital looking to implement a wearable technology.

Wearable cameras are typically used by security officers in a hospital. But they are equally as effective for nurses in home-care settings, because these professionals are completely on their own and don’t have the benefit of an installed base of network cameras around them the way a hospital has. Body-worn cameras work both ways, because they create a culture of accountability for all parties.

The goal of video surveillance in general — wearables especially — is to create a culture of accountability and transparency. This goal correlates with the American Nurses Association’s zero-tolerance policy against workplace violence. Wearables have the ability to complement de-escalation methods well due to the transparent nature of the technology. Success of a wearables program in a healthcare setting is embracing the balance of people, process and technology.

### IN-ROOM CAMERAS

One of the most interesting examples of technology aiding workflow optimization and surmounting staffing shortages is in the virtual nursing space. One form of virtual nursing is remote patient monitoring, also called “tele-sitting.” Another is for administrative purposes, using distributed communication in a patient’s room.

With remote patient monitoring, trained staff in a central location use clinical monitoring technology to observe patient activity in live-view. Very rarely — almost never — is the video or any associated audio recorded. A common example of this technology is monitoring patients who are deemed a fall risk. Another is monitoring patients who have behavioral health issues, such as those who exhibit a potential for self-harm.

Typically, in this scenario, there is a 12-to-one ratio of patients to care technician. The setup involves one-way video and two-way audio so the care technician can converse with patients to redirect them back to their bed or chair if necessary; technicians also can request bedside assistance.

Patient falls, which are the No. 1 cause of injury in a hospital, are not only expensive but they significantly degrade the patient experience when they happen. Some hospitals have reduced the incidence of falls by 80 percent after implementing live-view monitoring technologies.

As cameras became common in patient areas, clinical organizations expanded their use beyond remote patient monitoring. One key application is streamlining admissions and discharge processes, enabling healthcare teams — perhaps multiple nurses, an anesthesiologist, and a surgeon — to communicate effectively. This can enhance efficiency, save time, free up beds faster, and accelerate the patient’s stay.

Specific technologies contribute to this process and make it an immersive experience — for example, two-way video-based workflows. Pan-tilt-zoom cameras allow clinicians to read wrist bands and medication labels or monitor fluid drips. Typically, cameras operate in full resolution at 30 frames per second, with compression technology managing throughput.

Interoperable systems using the required privacy guardrails is another tool for improving workflow efficiency. As an example, the live video feed from a virtual nursing camera of a patient whose behavior is escalating could be diverted to the security department as an alert for possible de-escalation. Artificial intelligence (AI) is one of the technologies being used — analytics can blur certain features — in the trend towards interoperable systems.

### ARTIFICIAL INTELLIGENCE

AI is already a critical tool of modern medicine, and now it is becoming well-adopted at hospitals and often woven into the general workflow. For example, GPTs and similar technology helps with auto-charting, so healthcare professionals can spend less time writing and more time caring for patients. It pulls data fields from the medical record of a patient to partially populate a probable charting message.

In remote patient monitoring, AI is assisting care technicians by alerting to behaviors such as a patient’s leg going over the side of the bed or the lowering of a bed rail. Plotting a virtual box around the bed sets up for an alert when that “patient envelope” is broken. Getting alerts in real time is the gold standard in AI workflow.

AI also can be used in a more traditional security sense, perhaps generating an alarm based on a perceived behavior of an individual such as lingering in a spot they shouldn’t be or speaking aggressively. The technology can identify an individual who is registered on a watch list, so security can address the situation proactively.

Workflow optimization doesn’t necessarily have to incorporate an AI model. Improving efficiency could just as easily result from using traditional technologies such as lighting, signage, duress alarms, and two-way audio-video intercoms, as in a system installed at hospital entry points to comply with Laura’s Law.

When adopting emerging technologies such as AI, audio, and video to optimize workflows, healthcare organizations should prioritize open architecture and non-proprietary solutions with functional testing in their clinical environment. These enable interoperability across a healthcare site’s domains of safety, patient care, and operations, and offer high value to the organization. 🍷

# The Paxton Tech Tour

Your hot ticket to the security event of the year!  
Don't miss your chance to attend.



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

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



Easy to quote



Easy to install

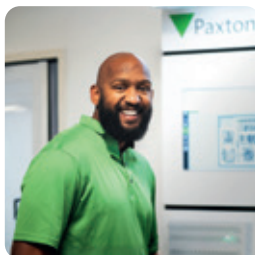


Easy to work with

Tech demos



Paxton product experts



Up to 80% off product



Exclusive installer gift



Free access control software



Got a question? Speak to our Paxton experts on  
(877) 438-7298 or email [PaxtonTechTour@paxton-access.com](mailto:PaxtonTechTour@paxton-access.com)

[paxton-access.com/us/tech-tour](http://paxton-access.com/us/tech-tour)

Get your free ticket today ►





# HOW TO HARNESS ALPR FOR GREATER SECURITY, EFFICIENCY AND COLLABORATION

BRUCE CANAL IS ACCOUNT EXECUTIVE LEAD—EDUCATION WITH GENETEC.

**W**ithin higher education campus environments, the demand for greater security, efficiency, and resources is ever-present. Many higher education teams are adopting advanced technologies to secure their campus, streamline operations, and continue to best serve their students and faculty. Automatic license plate recognition (ALPR) technology stands out for its ability to meet a wide range of campus objectives.

While traditionally ALPR solutions collect only information on the license plate, select ALPR solutions go beyond the license plate and collect data about vehicle characteristics. This may include details such as type, color, location, and speed. This complete data is a valuable campus resource for your campus.

Exploring the applications of ALPR reveals how you can bridge the gap between you and your parking and transportation counterparts. This connection can make your campus safer and more efficient.

## ALPR FOR CAMPUS SECURITY

Chances are you are already using video cameras to boost security in your campus parking lots and along busy roads. However, without ALPR, you lack the necessary context that could make a difference when responding to security threats.

Imagine someone driving off in a vehicle involved in an on-campus incident. The information gathered from the ALPR camera can collect the vehicle's license plate, color, and type. This information is then stored in the system's database. Security personnel now receive immediate alerts whenever ALPR cameras located throughout campus detect this vehicle of interest.

Witnesses can also give helpful leads but may struggle to remember specific details, especially license plate numbers. An ALPR system resolves this issue by allowing you to search the database based on characteristics such as vehicle type, color, and even partial plate numbers. This capability will enable you to efficiently narrow down vehicles of interest and enhance the effectiveness of your investigations.

Lastly, today's best ALPR systems can analyze the speed of a passing vehicle. This feature is invaluable from a campus safety perspective. Security personnel can monitor vehicle speeds in real time, allowing them to respond quickly to reckless driving behavior. If the system detects a vehicle speeding in a designated area, it can trigger an alert, allowing security to intervene promptly.



## ALPR FOR PARKING MANAGEMENT

As you advocate for ALPR technology, it's essential to communicate the dual benefits of enhanced security and improved operations. Start by working with your campus's parking department to determine any inefficiencies they may be experiencing.

For example, many parking systems rely on physical tags or decals that must be prominently displayed on vehicles. These tags or decals distinguish authorized vehicles from unauthorized vehicles within designated parking areas.

However, such traditional parking management methods are inefficient and costly. Physical permits often create administrative burdens, such as the need for regular renewals, permit distribution, and manual verification.

With ALPR for parking management, students, staff, and visitors are no longer burdened by manual processes. Drivers can register their vehicles online. They just need to enter their license plate number and vehicle details into the system. Once registered, vehicles are automatically recognized upon entering designated parking areas. Verification is then conducted via access control integration or mobile enforcement tools.

This self-service solution eliminates physical permits to reduce administrative burdens and overhead costs. Teams can further reallocate resources that were once allocated for visual parking verification. It also improves security by eliminating the possibility that someone will lose, steal, or share permits.

It's also possible your campus's parking and transportation department already uses ALPR. They may not realize that the same system can enhance campus security. At the same time, you and your team might be overlooking ALPR for applications beyond security. This gap in awareness is why communication is so important.

## THE VALUE OF CROSS-DEPARTMENT COLLABORATION

The main benefit of applying ALPR systems to enhance security and parking management is cost savings. Now, you and your campus's parking department can share the resources needed to implement and maintain the technology. This makes it simpler to justify the investment in ALPR technology.

Security teams gain access to valuable vehicle data that aids investigations and incident response, while transportation teams benefit from automated, more efficient parking enforcement.

The insights gained from ALPR data also prove invaluable for long-term planning and traffic management. Your campus can predict peak traffic by analyzing historical and real-time vehicle data. It can also optimize parking layouts and design more

efficient traffic routes. This forward-thinking approach improves the overall experience for those on campus.

Finally, consider how ALPR can strengthen your ties with local law enforcement. Police monitoring a vehicle linked to an incident off campus can rely on the campus's ALPR system to alert them if that vehicle appears on campus. Officers can respond quickly if the ALPR system detects a vehicle of interest. This potentially prevents further incidents and aids agencies in ongoing investigations.

#### EVALUATING ALPR SOLUTIONS

There are a few key considerations to keep in mind when selecting the right ALPR system for your campus.

- **Accuracy** - Can the cameras capture quality images in diverse weather and light conditions? Are the reads accurate from various angles? At what speeds can we gather accurate readings? These are all questions you should ask your solution provider.

- **Mobility** - High-quality solutions allow you to deploy mobile ALPR cameras. This means that a patrol vehicle can effectively enforce parking lots using ALPR cameras mounted on the exterior. Select ALPR solutions also offer mobile phone connectivity, converting your phone into a helpful enforcement tool. You can securely access your ALPR

system and verify parking permissions or hotlists while on the go.

- **Analytics and operation software** - Analytics provided at the edge deliver real-time insights. These analytics include plate numbers, vehicle type, color, date, time, and location. You'll also want easy-to-understand reports that enable you and your colleagues to use available data to make informed decisions.

- **Data privacy and security** - Look for a solution that encrypts data, stores it securely, and complies with privacy regulations. ALPR systems gather vehicle information but do not record personal identity details. Still, you should ensure transparency with stakeholders regarding how you use this data. You can do this either via posted signage or online policies.

#### SEEING BEYOND SECURITY

The future of campus security depends on breaking down the barriers between departments. ALPR systems are a great starting point for accomplishing this. Their ability to meet multiple campus objectives opens the door to enhanced security, efficiency, and collaboration. By applying ALPR technology across campus, you can enhance your situational awareness while improving the overall campus experience. ♥

# ULINE

## TECHNOLOGY STORAGE SOLUTIONS



COMPLETE CATALOG  
**1-800-295-5510**  
uline.com



**ORDER BY 6 PM FOR  
SAME DAY SHIPPING**



# HOW EMERGING TECHNOLOGIES ARE TRANSFORMING THE SCHOOL SECURITY LANDSCAPE

BRAD CARY IS BUSINESS DEVELOPMENT MANAGER FOR EDUCATION AT MILESTONE SYSTEMS.

Students can't focus on learning when they're worried about their safety. As education systems nationwide face evolving security challenges with limited resources, a new generation of integrated technology solutions is helping schools create safer environments while maximizing staff efficiency.

These evolving challenges require sophisticated approaches that go beyond traditional security measures. Today's emerging security technologies extend beyond conventional video cameras, offering powerful tools that provide real-time insights and proactive threat detection. At the heart of these solutions is the open platform video management software (VMS), which serves as a central hub connecting various smart devices and analytical tools.

## BRINGING INTELLIGENCE TO VIDEO SECURITY

While most schools have basic video systems, these are often used only after incidents occur. Today's data-driven video technology transforms this reactive approach into a proactive safety strategy. Modern open platform VMS solutions can integrate with intelligent video analytics to monitor, detect and classify objects and activities in real time. Rather than replacing human judgment, these systems serve as digital assistants, providing security teams and administrators with critical information to make faster, better-informed decisions.

These tools act as a force multiplier, allowing security personnel to monitor larger spaces more effectively while remaining alert to potential issues that require human intervention. AI-powered systems can learn to recognize out-of-ordinary situations, such as someone walking against normal traffic flow to objects left behind or a person lying on the ground. When unusual activity is detected, the system can immediately alert appropriate personnel via desktop computers, smartphones or other mobile devices.

While intelligent video systems provide visual insights, today's comprehensive security solutions extend beyond cameras alone. The integration of specialized sensors at the edge of the network significantly enhances a school's security posture. These smart devices serve as the eyes and ears of the security system, collecting vital data from throughout the campus. Multi-sensor devices offer an expanding range of capabilities:

When connected to an open platform VMS, these edge devices create a comprehensive awareness network. For example, when a keyword is detected by an audio sensor, the VMS can

automatically notify relevant personnel, display live video feeds, and initiate appropriate response protocols.

## CLOUD CONNECTIVITY ENHANCES FLEXIBILITY AND RESPONSE

Cloud-based and hybrid security solutions are also revolutionizing how schools approach video security. Recent improvements in national data infrastructure, coupled with advances in video compression and 5G wireless networks, have made cloud VMS options both feasible and affordable. The benefits of cloud connectivity extend far beyond simple remote access:

- Enhanced data sharing capabilities allow security teams to instantly share video information with first responders during emergencies
- Hybrid approaches combine on-premises equipment with cloud resources, offering scalability without abandoning existing investments
- Flexible payment models eliminate large upfront capital expenditures, allowing schools to scale their security infrastructure based on actual needs
- Infrastructure simplification reduces the need for extensive server rooms and complex maintenance schedules

Cloud connectivity is transforming how security teams collaborate with first responders. The ability to instantly share video data during emergencies enables faster and more coordinated responses to security incidents. This real-time information sharing can significantly improve outcomes during critical situations by giving emergency personnel vital situational awareness before they even arrive on scene.

## A HOLISTIC APPROACH TO SCHOOL SAFETY

The most effective school security strategies combine technology with thoughtful policies and procedures. While advanced tools provide powerful capabilities, their implementation must be part of a comprehensive security plan that addresses the unique needs and challenges of each campus.

Schools should consider privacy implications, obtain necessary permissions, and ensure technology is used ethically and responsibly. Transparent communication with students, parents, and staff about the purpose and limitations of security technology helps build trust and community support for these initiatives.

When properly integrated, these emerging technologies empower schools to do more with less—maximizing the effectiveness of security staff while creating learning environments where students and teachers feel safe and protected. 🛡️





**CAMPUS SECURITY**  
**TODAY**  
education | healthcare | corporate

# Expand your Knowledge and Explore.

Attend our **FREE** webinars on a  
wide range of topics.



[campussecuritytoday.com/webinar](https://campussecuritytoday.com/webinar)

AI

School Shootings

Cloud

Leadership

School Safety

Notification



## SECURING HIGHER EDUCATION:

## COMBATING ENROLLMENT FRAUD AND EMPOWERING STUDENT FINANCIAL SUCCESS

AUTHOR: BRIAN SUPONCIC IS SENIOR VICE PRESIDENT OF SALES AND CLIENT OPERATIONS AT BM TECHNOLOGIES (BMTX).

IMAGE: HAKINMHAN/STOCK.ADOBE.COM

**H**igher education institutions are facing a costly and growing crisis: enrollment fraud. Between 2020 and 2022, the cost<sup>1</sup> of acquiring a new student surged by up to 32%, straining already tight budgets. At the same time, “ghost students” using stolen identities to enroll fraudulently put institutions at even greater financial risk.

The rise of enrollment fraud not only threatens financial stability but also poses significant risks to campus security. As fraudulent actors infiltrate educational institutions through digital means, they potentially gain access to sensitive student data, campus resources, and even physical spaces. This breach of security extends beyond financial implications, raising concerns about the safety and privacy of legitimate students and staff. Campus security teams now face the dual challenge of protecting physical spaces and safeguarding digital identities. The ghost student phenomenon has evolved from a mere administrative issue to a critical security threat, demanding a comprehensive approach that integrates cybersecurity measures with traditional campus safety protocols.

Beyond the direct monetary losses, this wave of fraud is disrupting academic integrity. When schools unknowingly distribute aid to fake students, legitimate learners lose out. Inflated enrollment numbers lead to misallocated resources, making it harder for genuine students to access the courses they need to graduate. As institutions struggle to keep up, the quality of education and student success are in jeopardy because of this growing problem.

**WHEN FAKE STUDENTS COST REAL MONEY: GHOST STUDENTS**

Ghost students aren't just a financial burden but a growing digital threat. With open enrollment policies and minimal application barriers, community colleges have become prime targets for fraudsters using stolen identities and automated bots to exploit financial aid and institutional resources. In California alone, a shocking 20% of community college applications were flagged as fraudulent, with

the California State Chancellor's Office identifying 460,000 suspicious applications out of 2.3 million. The problem extends beyond California. According to the Chronicle of Higher Education, fraudsters sent 80 fake applications to Prince George's Community College in Maryland, submitting one every seven

minutes for hours, highlighting the scale and speed at which these digital attacks can occur.

Across the U.S., colleges and universities struggle to combat a surge in digital enrollment fraud, where cybercriminals manipulate weak security systems to enroll fake students at scale. Academic institutions risk financial losses, misallocated resources, and compromised student data without vigorous identity verification and digital safeguards. Higher education institutions must prioritize digital security as cyber threats evolve to protect their students, budgets, and integrity.

Enrollment fraud is not just an administrative headache; it's a financial and operational crisis that threatens the stability of higher education institutions. When universities unknowingly disburse financial aid to fraudulent applicants, these funds are rarely recovered, resulting in staggering economic losses. In California, Fullerton College identified \$1 million in financial aid payments that would have been lost to fraud had officials not halted them in time. This demonstrates the potential scale of losses for a single institution.

This escalating threat to campus security demands immediate action. Manual verification processes are now dangerously outdated due to increasingly sophisticated fraud tactics. Without adopting modern identity verification tools and digital safeguards, colleges and universities risk losing millions while jeopardizing the education of real students who deserve support.

**STRENGTHENING ENROLLMENT SECURITY IN HIGHER EDUCATION**

In the face of the growing threat posed by ghost students, universities are turning to cutting-edge identity verification technologies to safeguard the integrity of their enrollment processes. By harnessing the power of artificial intelligence and machine learning, institutions can uncover patterns of fraudulent activity that would otherwise remain hidden. These advanced tools not only detect inconsistencies in enrollment data, but they can also proactively prevent fraudulent actions, revolutionizing the way colleges protect their resources and students. This technological leap will significantly shift how higher education defends against threats.

Furthermore, implementing a streamlined, secure enrollment verification process goes beyond efficiency. It empowers universities to reallocate their time and resources to what truly matters: student success. During peak enrollment periods, the strain of manual verification can overwhelm admissions teams, draining valuable hours that could be better spent on supporting



students and enhancing educational outcomes. By adopting advanced digital solutions, institutions can significantly reduce the burden of time-consuming manual reviews, freeing staff to focus on strategic initiatives that foster student engagement, retention, and academic achievement. Higher education institutions could save an average of 15-20 hours each week during peak enrollment, enabling them to redirect their efforts toward shaping a more dynamic and supportive learning environment.

#### CHARTING THE STUDENT FINANCIAL ROADMAP

While preventing and reducing enrollment fraud is critical, it is equally important to consider the financial journey students embark upon once they step onto campus. For many students, college is the first time they open a bank account, viewing it as a key tool for managing student loans and daily living expenses. Without secure identity verification at the point of enrollment, fraudulent actors can gain access to the financial aid meant for genuine students, potentially derailing their financial path from the very start. By safeguarding student identities from day one, universities ensure that legitimate students receive the financial support they need, allowing them to build a strong foundation as they navigate their finances during college and after graduation.

Providing students with the right tools and knowledge to

manage their finances responsibly can leave a profound and lasting impact on their futures. Universities, in working with FinTech providers, have the opportunity to offer valuable financial literacy resources that empower students to make informed choices about their money. As students navigate the journey through higher education and into their careers, they often face new economic challenges, from paying off loans to managing their income and planning for the future. This transition period can be particularly demanding for students who balance work and studies simultaneously.

By equipping them with the right tools early on, universities and fintech providers can help students of all ages foster long-term financial health and empower them to build a secure financial future long after they leave the classroom.

As higher education continues to evolve, it's clear that tackling enrollment fraud and financial mismanagement requires a unified, proactive approach. By combining advanced identity verification technologies with a focus on financial literacy, schools can protect students, preserve the integrity of education, and ultimately shape a more equitable and resilient system. ♥

#### REFERENCE

1. <https://www.ruffalonl.com/blog/enrollment/3-key-takeaways-from-the-cost-of-recruiting-an-undergraduate-student-report/>





# HOW COMPOSABLE SECURITY TECHNOLOGIES FORTIFY CAMPUS SAFETY

DAVE BAKER IS SENIOR SOLUTIONS ARCHITECT AT LIVEVIEW TECHNOLOGIES (LVT).

Campus security teams have faced myriad risks threatening the safety and well-being of students and faculty this semester:

- Protests, which are common with any transition of power and legislative changes, bring heightened potential for altercations or infringement of First Amendment rights.
- Sports games and events can inspire energy that spirals out of control, making it challenging to contain situations and identify who is at fault if a fight or incident occurs.
- Bad actors rely on the cover of night to vandalize buildings, break into vehicles, or even commit arson.

Leaders have made tough tradeoffs about where to focus and how to channel limited resources to best protect their communities — but they now have a much-needed lift to their toolkit.

Rapid advancements in artificial intelligence (AI) have enabled powerful tools that offer essential capabilities to make the most of existing investments, deter potential incidents, and effectively pursue bad actors. Let's examine which technologies you should consider and how to stay resilient no matter what challenges you face.

## TECHNOLOGIES IMPROVING SCHOOL SAFETY

Today's campus environment is wrought with disparate technology systems that do not communicate with each other, which greatly hampers efficiency (and wastes money).

The key to building a resilient campus security strategy is to connect disparate systems. Composable systems achieve this vision, in which every tool can connect and relay information back to a centralized platform.

Security teams need aggregated insights to make fast, informed decisions. It is not effective to use standalone systems for intrusion detection, door locks, and cameras — every tool needs to be composable so it can communicate with the entire ecosystem.

The following solutions have proven especially valuable as part of a connected security ecosystem:

- **AI-powered security cameras:** Cameras are no longer effective if they only record environments. Video camera solutions need to provide metadata on the objects they detect so teams can get ahead of potential threats. Active shooter scenarios, although rare, and similar attacks underscore the need for camera systems to proactively alert teams if a weapon is identified on campus. Time saves lives in urgent scenarios, so intelligent cameras

that identify weapons can decrease response times and empower first responders with valuable information.

- **Body cameras:** Detailed evidence is vital for preserving truth. Body cameras are increasingly used to support incident review and provide objective evidence of an incident.

- **Loudspeakers:** Speakers can connect to other security solutions and trigger customized announcements or personalized warnings, demonstrating a strong security posture. Speakers can also trigger loud alarms that draw attention to an area when an incident occurs.

- **Mobile security systems:** Stationary cameras are not the only option for surveying areas. Drones and even robot dogs can be deployed to expand coverage and follow bad actors as they attempt to flee an area. These technologies offer a unique vantage point and provide the necessary flexibility for certain scenarios.

Each of these may be a valuable addition to your safety toolkit. At a minimum, check with your existing providers to understand what features you may be underutilizing and how to connect the solution with your other tools.

## BRINGING STUDENTS INTO THE SAFETY CONVERSATION

Students deserve to feel safe on campus. However, they may not know about the resources available to them, and they may be skeptical about new technologies or a perceived increase in security personnel.

Campus leaders should educate students and faculty on the measures in place to protect them and how each solution works:

- Overview common safety threats and provide resources to navigate potential safety concerns.
- Discuss what technology your security team uses and invite questions to dispel misconceptions, like whether facial recognition is used or if students are "being tracked."
- Celebrate safety wins and acknowledge how your team has addressed situations swiftly.

## KEEPING PACE WITH EVOLVING CAMPUS SECURITY THREATS

The security world must embrace composability and connected solutions. Otherwise, valuable information will be lost or require too much time to aggregate. Full, connected information from security systems makes it easier to glean insights, fortify weaknesses, and share information from campus to campus.

By continually testing new capabilities and leveraging AI to its fullest potential, campus leaders can tackle any new challenges in stride. 🛡️



# Clean hard-to-reach campus cameras with ease.



The **ProSeries 25'** and **ProSeries 40' Max** are designed for professionals who need exceptional reach, durability, and performance.

## POPULAR ProSeries 25'

Perfect for medium to large camera installations in schools, airports, casinos, etc.

PN: DW-PKG-25-BL

## ECO DomeWizard COMPACT 13'

Ready for on-the-go maintenance of camera domes and enclosures that are just out of reach.

PN: DW-COMPPKG-13

## MAX ProSeries 40'

The ultimate solution for high hard to reach places in stadiums, warehouses, traffic areas and airports.

PN: DW-PKG-40-BL

**Extended reach:** Clean high installations without ladders or lifts.

**Premium build:** Lightweight carbon fiber poles for easy handling at full extension.

**Efficiency boost:** Reduce cleaning time by covering more area in one go.

**Professional maintenance:** Combine our **4-in-1** cleaning for improved camera performance.

**Exceeds OSHA & Insurance Carriers' Safety Mandate:** Protects workers by eliminating the need for ladders, scissor lifts, or risky high-altitude work, ensuring compliance with safety regulations.

## How to order

Visit our website: [www.dotworkz.com](http://www.dotworkz.com)

Call us directly: (866) 575-4689

Email us: [sales@dotworkz.com](mailto:sales@dotworkz.com)

Bulk purchasing + OEM

Take cleaning to new heights - order your **ProSeries 25'** and **ProSeries 40' Max** today!

Scan

For more  
DomeWizard  
information





See What You've Been Missing:

## With New Marks Indicator Locks, *You'll Know The Campus Is Safe*

### SKA500 Series

Marks High-Visibility Indicator Lock Series  
Instant Lock Status at a Glance – Safety & Security Made Simple

- **Red Means Locked, Green Means Unlocked** – Highly visible indicators provide clear door status, ensuring confidence and peace of mind for occupants.
- **Easy Installation with Marks 5 Series Grade 1 Mortise Locksets** – Mounted independently or combined to be double-sided. Available in Turnpiece-TP, Coin Key -CK or Cylinder -CYL models
- **Intuitive & Hassle-Free Operation** – No guesswork—occupants and staff instantly know if the door is secured.
- **Enhanced Safety for Schools, Healthcare, & Businesses** – Quickly assess room security in critical moments, improving emergency response and daily operations.
- **Code-Compliant & ADA-Friendly** – Designed for ease of use, meeting security & accessibility requirements across various applications.
- **Trusted Durability from a Locking Industry Leader** – Backed by Marks' decades-long reputation for quality, reliability, & performance & Lifetime Warranty
- **Ideal for High-Use Areas** – Perfect for classrooms, patient rooms, lounges, offices, and more, ensuring clarity and security in busy environments.



### Marks Status Indicator Series



(shown left to right)  
Cylinder -CYL, Coin Key -CK & Turnpiece-TP models



Now Available at the Marks Distributor Near You



# MARKS USA

1.800.645.9445 [www.marksusa.com](http://www.marksusa.com)

Marks USA a Division of Napco Security Technologies, Inc., Amityville NY 11701 USA,  
Prelim Data Subject to change without notice.