MARCH 2026 | ISC WEST HANDBOOK

www.securitytoday.com
SECURITY today
Technology | Education | Solutions

ISC WEST HANDBOOK

SHOWCASING NEXT GENERATION TECHNOLOGIES OF PHYSICAL SECURITY

Handbook Patrol

Every year, the security industry looks to ISC West in Las Vegas as a preview of the technologies that will define the next generation of physical security. The 2026 exhibition, taking place March 25–29, continues this tradition by showcasing innovations designed to better protect people, property, and critical assets in an increasingly complex threat environment.

One of the most visible trends on the show floor is the evolution of AI-driven video analytics. Modern surveillance systems are moving far beyond simple motion detection. Today's platforms leverage artificial intelligence to identify unusual behavior, detect perimeter breaches, recognize vehicles, and even analyze crowd movement in real time. These capabilities allow security teams to shift from reactive monitoring to proactive threat prevention, reducing response times and improving situational awareness across campuses, facilities, and public venues.

Another area gaining momentum is the integration of cloud-connected security infrastructure. Cloud-based access control, video management systems, and alarm monitoring solutions provide organizations with the ability to manage multiple locations from a single interface. For security professionals responsible for distributed facilities—such as healthcare networks, school districts, corporate campuses, or energy sites—this centralized visibility is transforming how security programs are operated. Updates, system diagnostics, and data access can be handled remotely, improving efficiency and reducing maintenance costs.

Advanced access control technologies are also evolving rapidly. Biometric authentication methods such as facial recognition, fingerprint scanning, and mobile credentialing are becoming more accurate and easier to deploy. These systems provide a balance between strong security and user convenience, allowing authorized personnel to move seamlessly through secured areas while preventing unauthorized access.

In addition, the show highlights a growing focus on integrated security ecosystems. Rather than operating as isolated tools, modern security technologies are increasingly designed to communicate with one another. Video surveillance, intrusion detection, access control, and emergency notification systems can now share data across unified platforms. This integration enables security teams to gain a comprehensive view of events as they unfold, improving coordination during incidents and supporting more informed decision-making.

Another emerging theme at ISC West is the use of edge computing and intelligent devices. Cameras and sensors are becoming smarter, processing information locally before sending relevant alerts to centralized systems. This approach reduces bandwidth demands and allows for faster detection of potential threats, particularly in large-scale environments like airports, manufacturing facilities, and transportation hubs.

Ultimately, the innovations featured at ISC West reinforce a central goal of the physical security profession: protecting life, safeguarding property, and preserving operational continuity. By combining artificial intelligence, cloud connectivity, biometric authentication, and integrated system design, the technologies on display represent a significant step forward in how organizations prepare for and respond to evolving security challenges.

RALPH C. JENSEN
Editor-in-Chief, *Security Today* magazine

Table of Contents

MASS NOTIFICATION
3 **Why Mass Notification is on the Rise, and Why Integrators Should Care**

VIDEO STORAGE
5 **Rethinking Long-Term Video Storage for Modern Security**
How cloud-based archiving helps enterprises retain more video while reducing cost and complexity.

UNIFIED ARCHITECTURE
7 **From Fence Lines to Federated Identity**
Why modern government security demands unified architecture from edge to identity

COMMUNITY SURVEILLANCE
9 **Lancaster Builds Safe City with Video Technology**
Pennsylvania city transforms crime-ridden streets through community video surveillance

WEAPONS DETECTION
11 **Athena Is Preparing Entryways for Mandates Like AB 2975**
Why Hospital Visitor Management Systems and Concealed Weapons Detection Must Work Together

13 **Product Spotlights**
A collection of security solutions.

Why Mass Notification is on the Rise, and Why Integrators Should Care

BY GINA SANSIVERO

Mass notification has moved from "nice to have" to mission-critical. Schools, campuses, enterprise offices, hospitals, airports, and municipalities are upgrading systems to reach people instantly—on any device, in any space—when seconds matter. For security integrators, this shift represents one of the most attractive growth markets: platform sales, endpoints, services, and multi-year support contracts all bundled into high-value projects.

What's driving demand, how do you position your offerings, and where does margin live?

What's driving the surge in projects?

1) Heightened duty of care and compliance. Organizations face stronger expectations to warn, inform, and guide occupants during threats, severe weather, and operational disruptions. Many verticals now reference standards that emphasize audibility/intelligibility, auditable alerting, and multi-channel reach. That pressure is translating into funded initiatives with clear timelines.

2) Hybrid, distributed environments. Workplaces and campuses aren't single buildings anymore. They're a mix of classrooms, labs, residence halls, arenas, remote offices, and outdoor spaces, with people on the move. Customers need IP-based, multi-modal alerting (audio, strobes, desktop takeover, SMS, SIP phones, mobile apps) that can target zones or go site-wide in seconds.

3) Convergence of AV, IT, and physical security. Mass notification sits at the intersection of paging/PA, VMS, access control, fire/life safety, and collaboration platforms. Customers want a unified workflow: trigger → approve → reach everyone. Interoperability is no longer a feature; it's a requirement, and integrators who can stitch systems together win.

4) Mature, scalable technology. Modern platforms are easier to deploy, centrally managed, and analytics-ready. IP endpoints, PoE power, and standards-based integrations reduce friction. Cloud dashboards make health monitoring and content updates simpler for facilities and security teams.

5) Funding windows and risk reduction ROI. K-12, higher ed, healthcare, and public sector buyers can often access grants or budget carve-outs tied to safety and emergency preparedness. Framing projects around measurable risk reduction and continuity planning helps unlock these funds.

Why should integrators care?

Bigger deals, faster cycles. Bundling the platform with endpoints (IP speakers/displays), amplifiers, networked controllers, and accessories creates a complete solution. Add design, commissioning, and training, and you have a turnkey package that expedites approvals.

Recurring revenue and account stickiness. Mass notification is not "sell and leave." Monitoring, testing, message management, content updates, cybersecurity patching, and periodic re-intelligibility checks all support SLAs. That means multi-year contracts and predictable services revenue.

Clear differentiation. Many bids still underweight audio. Lead with intelligibility metrics (STI/CIS), targeted zoning, and scenario-based workflows. Demonstrate integration with access control, VMS, and IT alerting tools. Show how operators can launch the right message in under 10 seconds.

Cross-sell pathways. Once a mass notification backbone is in place, customers expand zones, add outdoor coverage, enable desktop/mobility, and standardize other venues. One successful site often turns into a programmatic rollout.

What does "good" look like? (buyers will ask)

Intelligibility, not just audibility. End users increasingly evaluate speech clarity, not volume. Design to STI targets for each space type and document results. Distributed audio with proper directivity beats "shout from the front" every time.

Multi-modal, multi-channel delivery. Reach people through IP endpoints, LEDs, strobes, SMS, desktop pop-ups, SIP phones, and collaboration tools. Support pre-recorded and live paging, bilingual messaging, and role-based approvals.

Interoperability and open interfaces. Look for platforms that integrate with access control, VMS, fire panels, and building systems via standards (SIP, REST, GPIO, SNMP). Fewer "one-off" bridges make projects more maintainable.

Speed, simplicity, and role design. Operators need one screen, with plain-language scenarios: Lockdown, Evacuate, Shelter-in-Place, All Clear. Drill down by campus, building, floor, or zone. Make it impossible to do the wrong thing in a stressful moment.

Security and uptime. IT teams will scrutinize hardening, patch cadence, user provisioning, TLS, and logging. Plan for redundancy (server/cluster options), failover paths, and routine testing to prove readiness.

Lifecycle services. Bake in routine system testing, content reviews, software updates, and periodic intelligibility reassessments. This is where your SLA value is obvious and renewal is natural.

Gina Sansivero is the Vice President of Marketing & Corporate Communications at AtlasIED.

LEARN MORE:

If you want to see how a modern, interoperable mass notification platform comes together—and how to package it profitably—**schedule a 15-minute demo**.

DETECT, INFORM, MANAGE

AtlasIED Mass Communication Solutions offer the software and hardware necessary to easily and quickly detect risks, inform students, faculty and staff, and manage communications to first responders, community members, and off site stakeholders.

AtlasIED

Check us out at AtlasIED.com or engage with us on your favorite social platform

Rethinking Long-Term Video Storage for Modern Security

How cloud-based archiving helps enterprises retain more video while reducing cost and complexity.

BY OWAIS KHALID

As video retention requirements continue to grow, many organizations are discovering that traditional storage models are no longer sustainable. Banks, retailers, QSRs, and multi-site enterprises are being asked to retain video for years instead of weeks—driven by compliance mandates, liability protection, and evolving investigative needs. Yet extending retention has historically meant expanding on-prem infrastructure, absorbing rising hardware costs, and increasing IT overhead.

Long Term Cloud Storage is changing that equation.

Rather than treating video retention as a constant infrastructure expansion problem, modern cloud-based archiving allows organizations to store more video for longer periods without continually adding hardware. This shift is especially important as video data volumes accelerate due to higher camera resolutions, broader coverage areas, and a growing reliance on video as both a security and operational tool.

The challenge with traditional on-premise storage is not just cost, but rigidity. Organizations must forecast future capacity, purchase hardware upfront, and manage refresh cycles, power, cooling, maintenance, and backup processes over time. Scaling becomes slow and capital-intensive. Even archived footage that is rarely accessed must still be powered, protected, and maintained.

Long Term Cloud Storage introduces a more flexible model. Video can be retained securely offsite in cost-efficient archive tiers, while short-term or frequently accessed footage remains locally accessible. This tiered approach aligns storage costs with how video is actually used and how often it needs to be retrieved.

This tiered approach enables organizations to reduce long-term video storage costs by up to 80% over five years, while maintaining secure access to archived footage.

March Networks' Long Term Cloud Storage solution supports this hybrid strategy. Rather than requiring a full migration, it allows customers to maintain immediate access to recent video on-premise while archiving older footage in the cloud. The result is greater scalability, lower total cost of ownership, and reduced operational complexity.

At the core of this approach is tiered cloud storage powered by Amazon S3 Glacier. Designed for long-term data retention, Amazon S3 Glacier delivers ultra-low-cost storage with enterprise-grade durability and security. By shifting older video into archive tiers, organizations can avoid repeated hardware upgrades and reclaim valuable data center resources. Costs that traditionally existed as separate line items (hardware, power, cooling, rack space, backups, and maintenance) are consolidated into a predictable cloud service model.

Traditional on-premise storage can drive video retention costs higher due to ongoing IT overhead, maintenance, and hardware life cycle replacement. One customer using on-premise storage for immediate access to recent video evaluated March Networks Cloud Storage to extend video retention without adding new hardware.

For 580 cameras generating approximately 5,600 TB of archived video, the cloud storage costs were an estimated $347,000 per year, compared to approximately $1.7 million to store the same volume of video on-premise. This hybrid solution made recent footage instantly available while significantly reducing long-term video retention costs.

This model is particularly valuable for regulated industries. Financial institutions often retain video for years to support investigations and audits. Retailers and QSRs rely on long-term video to address liability claims, fraud investigations, and recurring safety issues that may only surface over time. In many of these scenarios, immediate access is not required, but having reliable, secure retention is essential.

Cloud-based archiving also strengthens resilience. Offsite storage provides protection against data loss caused by hardware failure, site-level incidents, or natural disasters. Built-in redundancy and durability on the other hand, help ensure archived video remains secure and available when needed.

Equally important, long term cloud storage reduces operational strain. IT teams are no longer responsible for forecasting years of storage growth or managing aging infrastructure. Storage scales elastically as needs expand, without disrupting operations. For organizations managing thousands of cameras across hundreds (or thousands) of locations, this simplicity can be just as impactful as the cost savings.

Long-term video retention should not stand in the way of modernization. With the right hybrid cloud strategy, organizations can meet compliance requirements, protect against liability, and preserve critical evidence without expanding infrastructure or escalating budgets.

As video continues to play a central role in security and operations, rethinking how it's stored is no longer optional. Long Term Cloud Storage offers a scalable, economically sustainable path forward that reflects how modern enterprises use video today.

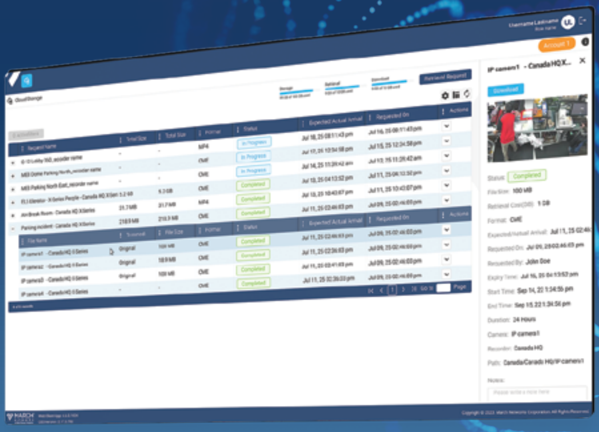
__Owais Khalid__ is a Senior Product Manager at March Networks, based in Ottawa, who leads the Enterprise Management and VMS portfolio.

LEARN MORE:

Learn more about March Networks Long Term Cloud Storage and how tiered cloud archiving can extend your organization's retention by visiting **marchnetworks.com** or connect with the team at ISC West at Booth 23035.

Vision and Intelligence. Aligned.

VISIT US AT ISC WEST.



Request Name	Total Size	Total Size	Format	Status	Expected/Actual Arrival	Requested On	Actions
6-10 Lobby 360_recorder name	-	-	MP4	In Progress	Jul 18, 25 08:11:43 pm	Jul 16, 25 08:11:43 pm	
MB Dome Parking North_recorder name	-	-	CME	In Progress	Jul 17, 25 10:34:58 pm	Jul 15, 25 12:34:58 pm	
MB Parking North East_recorder name	-	-	CME	In Progress	Jul 14, 25 11:26:42 am	Jul 13, 25 11:26:42 am	
F1 Elevator - X Series People - Canada HQ X Series	5.2 GB	5.3 GB	CME	Completed	Jul 13, 25 04:13:52 pm	Jul 11, 25 04:13:52 pm	
Air Break Room - Canada HQ X Series	31.7 MB	31.7 MB	MP4	Completed	Jul 13, 25 10:43:07 pm	Jul 11, 25 10:43:07 pm	
Parking incident - Canada HQ X Series	218.9 MB	210.9 MB	CME	Completed	Jul 11, 25 02:46:03 pm	Jul 09, 25 02:46:00 pm	

File Name	Transcod	File Size	Format	Status	Expected/Actual Arrival	Requested On	Actions
IP camera1 - Canada HQ X Series	Original	100 MB	CME	Completed	Jul 11, 25 02:46:03 pm	Jul 09, 25 02:46:00 pm	
IP camera2 - Canada HQ X Series	Original	18.9 MB	CME	Completed	Jul 11, 25 02:36:03 pm	Jul 09, 25 02:46:00 pm	
IP camera3 - Canada HQ X Series	Original	100 MB	CME	Completed	Jul 11, 25 03:41:03 pm	Jul 09, 25 02:46:00 pm	
IP camera4 - Canada HQ X Series	-	-	CME	Completed	Jul 11, 25 02:36:03 pm	Jul 09, 25 02:46:00 pm	

IP camera1 - Canada HQ X...

Status: Completed
File Size: 100 MB
Retrieval Cost(GB): 1 GB
Format: CME
Expected/Actual Arrival: Jul 11, 25 02:46
Requested On: Jul 09, 25 02:46:03 pm
Requested By: John Doe
Expiry Time: Jul 16, 25 04:13:52 pm
Start Time: Sep 14, 22 1:34:56 pm
End Time: Sep 15, 22 1:34:56 pm
Duration: 24 Hours
Camera: IP camera1
Recorder: Canada HQ
Path: Canada/Canada HQ/IP camera1
Notes:
Please write a note here

Copyright © 2025 March Networks Corporation. All Rights Reserved.

VIVOTEK
A Delta Group Company

Chroma24

FULL-COLOR VIDEO.
DAY AND NIGHT.

Delivers 24/7 reliable, full-color video without infrared or white light. Built for low-light and always-on environments.

BOOTH 22043

MARCH® networks
A Delta Group Company

Long Term Cloud Storage

STORE MORE VIDEO.
SPEND LESS. STAY IN CONTROL.

Extend video retention without adding infrastructure. Combine fast access on-prem with cost-efficient cloud archiving. Retain more video at up to 80% less cost.

BOOTH 23035

Smarter cameras. Smarter storage.
Built to scale together.

From Fence Lines to Federated Identity

Why modern government security demands unified architecture from edge to identity

BY SCOTT ELLIOTT

Government security leaders are operating in one of the most complex threat environments in modern history.

Physical threats are evolving. Compliance frameworks are tightening. Hybrid work has redrawn operational boundaries. Critical infrastructure is increasingly software-defined. And modernization must occur without disrupting mission continuity.

Yet in many public sector environments, security architecture still reflects a different era.

Perimeter detection was added after a breach. Access control upgraded to meet a standard. Video expanded after an incident.

Intrusion layers deployed for compliance.

Each solution solved a problem. Few were designed as part of a unified strategy. That fragmentation is no longer sustainable.

Fragmentation rarely fails loudly. It fails in the gaps.

A perimeter alert triggers, but isn't immediately contextualized with video. A credential is used unexpectedly, but identity context isn't visible within the same workflow. Operators swivel between consoles, losing seconds that matter.

These are not technology failures. They are architectural failures.

In high-consequence government environments — defense facilities, courthouses, transportation hubs, energy substations — the issue is rarely that systems are not working. The issue is delayed correlation between systems that are working independently.

Seconds matter. Context matters. Audit trails matter.

Without centralized visibility, response time increases, false alarms multiply and compliance reporting becomes reactive rather than operational. Leadership lacks enterprise oversight, and security teams are forced to assemble situational awareness during an incident rather than relying on systems designed to deliver it.

LEARN MORE:

Visit **hirschsecure.com** to learn how Hirsch unifies perimeter protection, intrusion detection, access control, video intelligence, identity, and integrations into one intelligent security ecosystem — delivering clarity, control and confidence for critical infrastructure, government and enterprise environments worldwide.

Modern security platforms must provide clarity before an event escalates, not after.

Compliance requirements are raising the bar even further. Government environments operate under strict frameworks such as CJIS, FISMA, FICAM, NIST-FIPS and NERC CIP. Increasingly, these mandates extend beyond physical security and into broader cyber-physical convergence.

Compliance today is not just about installing protection. It is about proving control.

Fragmented systems undermine that proof in several ways. Audit trails become inconsistent. Policy enforcement becomes disjointed. Data correlation becomes manual.

As Zero Trust principles expand beyond IT and into physical environments, organizations must continuously verify identities, enforce least-privilege access and maintain clear chain-of-custody records for security events.

This requires a shift in thinking — from integration to unification.

For many years, the industry's answer to fragmentation was integration. Systems were connected through APIs, middleware and custom connectors between vendors. Integration helped. But it preserved complexity.

Unification goes further.

Unification aligns detection, verification, access control, video intelligence and identity policy within a single operational architecture designed to work together from the beginning.

Integration connects systems. Unification aligns decision-making.

For government agencies, this distinction has practical operational benefits.

When a perimeter alert triggers, associated video should automatically load. Credential activity in nearby zones should appear in context. Identity information should be visible in the same interface. Response workflows should activate automatically.

Events are no longer isolated signals. They become part of a coordinated narrative.

This approach also enables centralized oversight across distributed estates. Government facilities are rarely concentrated in a single location. They span federal campuses, municipal offices, substations, remote infrastructure sites and transportation networks.

Unified platforms create a single source of truth while preserving the flexibility required for local operations.

At the same time, security infrastructure itself is evolving. Modern environments are increasingly networked, identity-driven and software-defined. The perimeter is no longer just fencing and gates. It includes connected devices, contractor credentials, remote operations and federated identity ecosystems.

Modern threats rarely begin — or end — at a single door.

Security failures increasingly occur in the handoffs between systems: between detection and verification, between access control and identity, between physical and cyber response teams.

A unified perimeter-to-identity architecture closes those gaps.

Detection, video verification, access enforcement, identity authentication and response workflows operate as coordinated layers rather than isolated technologies.

This model also supports the growing convergence between cyber and physical security. Identity is rapidly becoming the control plane of both domains. Hardware-backed authentication, multi-factor verification and policy-driven access governance are now central to security resilience.

For government organizations working within legacy infrastructure and long procurement cycles, modernization cannot rely on disruptive rip-and-replace strategies.

It enables agencies to align existing systems into a coherent operational framework, reduce complexity and strengthen resilience without compromising mission continuity.

The question for security leaders is no longer simply which system should be upgraded next. It is how the entire security architecture works together.

It is foundational.

__Scott Elliott__ is Chief Revenue and Marketing Officer at Hirsch, where he leads global revenue strategy, brand development and go-to-market initiatives for unified security solutions.

Lancaster Builds Safe City with Video Technology

Pennsylvania city transforms crime-ridden streets through community video surveillance

BY SAM PHILLIPS

By the late 1990s, Lancaster, Pennsylvania, had reached a tipping point. Crime had crippled the downtown area, businesses were shuttering, and residents who stayed no longer felt safe in their own neighborhoods. Witnesses stayed silent out of fear, creating a vicious cycle where crimes went unsolved and public trust eroded.

Then-Mayor Charlie Smithgall convened the Lancaster Crime Commission, bringing together business leaders and residents determined to take back their community. This grassroots collaboration evolved into the Lancaster Safety Coalition (LSC), a nonprofit organization that would deploy one of the nation's most innovative community-supported video security networks.

Building a Scalable Foundation

The Coalition's early video security efforts relied on digital video recorders and analog PTZ cameras that couldn't scale to meet the city's needs. Coverage gaps persisted, and the technology often failed to provide the reliable evidence law enforcement required. The LSC needed a flexible, future-proof solution.

The answer came through Milestone XProtect open platform video management software. Its open architecture allowed the Coalition to integrate best-in-class components from multiple manufacturers, creating a system that could adapt to new challenges.

Systems integrator App-Techs designed a deployment featuring approximately 170 4K quad-sensor cameras from i-PRO, strategically positioned throughout Lancaster's neighborhoods and downtown. Each camera generates four video streams, creating approximately 680 total streams operating around the clock.

LEARN MORE:

To learn more about how open platform video technology can transform community safety, please visit **Milestone Systems**, **Video Security** for Public Safety, or contact us directly through these **options**.

"When we got involved, we saw an opportunity to develop a system that could truly scale with their needs," explains Dan Fritsch, President of App-Techs. "We've built a solution with 12 recording servers, a failover server, and a management server, all optimized to handle the extraordinary volume of data throughput these cameras generate."

The infrastructure extends beyond typical surveillance deployments, with App-Techs managing a fiber network and 10-gigabit backhaul. The company developed proprietary Health Utility Monitor software that continuously monitors all system components, enabling proactive response to technical issues.

Measurable Impact on Crime and Investigation

The results speak clearly. Annual homicides plummeted from 10 to 15 down to just two. Video evidence availability soared from 55% to over 90%. In 2023 alone, LSC operators provided live video support to 911 dispatchers during more than 4,100 incidents.

The system operates as a force multiplier for local police. Officers frequently collaborate with LSC operators on high-level activities, including drug investigations and warrant service. While law enforcement regularly visits the LSC office to review video evidence, they cannot directly access or control the system, maintaining the Coalition's independence as a community organization.

App-Techs created a digital evidence delivery system that allows LSC operators to securely transfer video evidence to law enforcement through a browser-based interface while maintaining chain-of-custody protocols.

Investigation dynamics have fundamentally changed. Operators can track suspects across multiple camera views throughout the city. In one remarkable case, LSC operators tracked a shooting suspect from the crime scene back to their residence within 15 minutes, leading to an immediate arrest.

A Community Reclaimed

Beyond crime statistics, Lancaster's transformation is visible in its revitalized downtown. Streets once empty after business hours now bustle with activity.

"When other communities come in looking at our success, they always want to talk about money and cameras. I tell them your first step is determining, as a community, you've had enough. Because if you can't coalesce around the notion that you've had enough of how it's been, you can't make it into something different," says Tim Miller, Executive Director of LSC. "If you go downtown now on most any day of the week, the restaurants and businesses are hopping. There are people out taking ownership of the community again, and that's really great to see."

"What makes this project remarkable is the synergy between the technology partners and our community vision," Miller emphasizes. "The open platform from Milestone, the technical expertise from App-Techs, and our community-driven approach created a formula that's yielded extraordinary results. We've seen crime rates plummet, businesses return to downtown, and most importantly, neighbors reclaim their streets. This isn't just about cameras; it's about using the right tools with the right partners to empower a community."

Lancaster's transformation demonstrates that effective public safety requires more than technology. It demands community commitment, strategic partnerships, and the right technological foundation. For cities facing similar challenges, Lancaster offers a proven blueprint combining citizen engagement with open platform video technology.

***Sam Phillips** is Public Safety Lead at Milestone Systems, where he works with law enforcement and municipalities on video technology solutions.*

milestone

We built a time machine

What does the future of video security look like?

Visit us at ISC West 2026 in Las Vegas to find out. We'll be showcasing the open-platform adaptability needed to future-proof your security systems. You can also see our vision for responsible AI brought to life, and ready to use.

Stop by Booth #18053 and See Tomorrow

Athena Is Preparing Entryways for Mandates Like AB 2975

Why Hospital Visitor Management Systems and Concealed Weapons Detection Must Work Together

BY CHRIS CIABARRA

Security leaders across healthcare systems, schools, and public venues are facing a new reality at the front door. Healthcare workers are five times more likely to experience workplace violence injuries than workers in other industries, according to the U.S.

Entryways that were once designed primarily for visitor flow are now expected to serve as the first line of defense against increasingly complex threats. At the same time, legislation and workplace safety expectations are raising the bar for how organizations must protect staff and document their prevention efforts.

State governments are increasingly examining workplace violence prevention requirements in healthcare settings. California's Assembly Bill 2975 illustrates how expectations around hospital safety programs are evolving. The law requires hospitals in California to strengthen workplace violence prevention plans and implement screening measures designed to reduce risks at facility entrances.

For healthcare organizations evaluating how to prepare for these evolving expectations, the focus is shifting from responding to incidents after they occur to preventing risk before it enters the building—and that prevention begins by answering two questions at the front door: who is entering the facility, and what might they be carrying?

Weapons detection answers one critical question: Is someone carrying a weapon right now?

Visitor management answers equally important questions: Who is this person? Have they been involved in prior incidents? Should access be restricted, supervised, or documented? Are they authorized to be in the building today?

When these two layers work together, organizations gain a far more complete picture of risk at the front door.

Historically, these technologies have often been deployed separately. Visitor management systems verify identity, log guests, and issue badges, while weapons detection technologies screen for firearms, knives, and other threats at entry points.

Operating them independently can create gaps. Alerts generated by screening devices may exist as isolated events, and visitor records may not be linked to security incidents. In high-volume environments like hospitals, this fragmentation can slow investigations and complicate compliance documentation.

An integrated entryway platform like Athena Security addresses these challenges by linking visitor identity with screening results in real time. In a modern workflow, visitors first check in through a visitor management system that verifies their identity and records their presence. They then proceed through weapons detection screening before entering the facility.

When both processes operate within a coordinated platform, screening events are automatically associated with the visitor's record. Security personnel gain immediate visibility into both identity and threat information before the individual enters sensitive areas of the facility.

Research highlights how important this screening layer can be. A systematic review of hospital weapons screening programs found that approximately 4% of individuals screened at healthcare facility entrances were carrying a weapon, according to a 2024 study published in the National Library of Medicine.

Integration also enables a more proactive approach to safety. If a visitor previously triggered a weapons alert, caused a disturbance, or required intervention, that event can be linked to their profile and the system can automatically flag the record so staff can apply enhanced screening procedures, require an escort, or restrict access according to hospital policy.

Integrated systems also simplify reporting and compliance documentation. Hospitals must demonstrate how they track incidents, enforce policies, and maintain oversight of security programs. When visitor management and weapons detection operate together, organizations can generate unified reports that connect screening events, visitor records, and incident histories within a single system.

Operational efficiency is another important advantage. Hospitals must balance safety with compassion and accessibility while processing large numbers of visitors each day. Integrated entryway systems help maintain that balance by streamlining workflows through digital check-in, badge printing, automated visitor limits, and coordinated screening procedures.

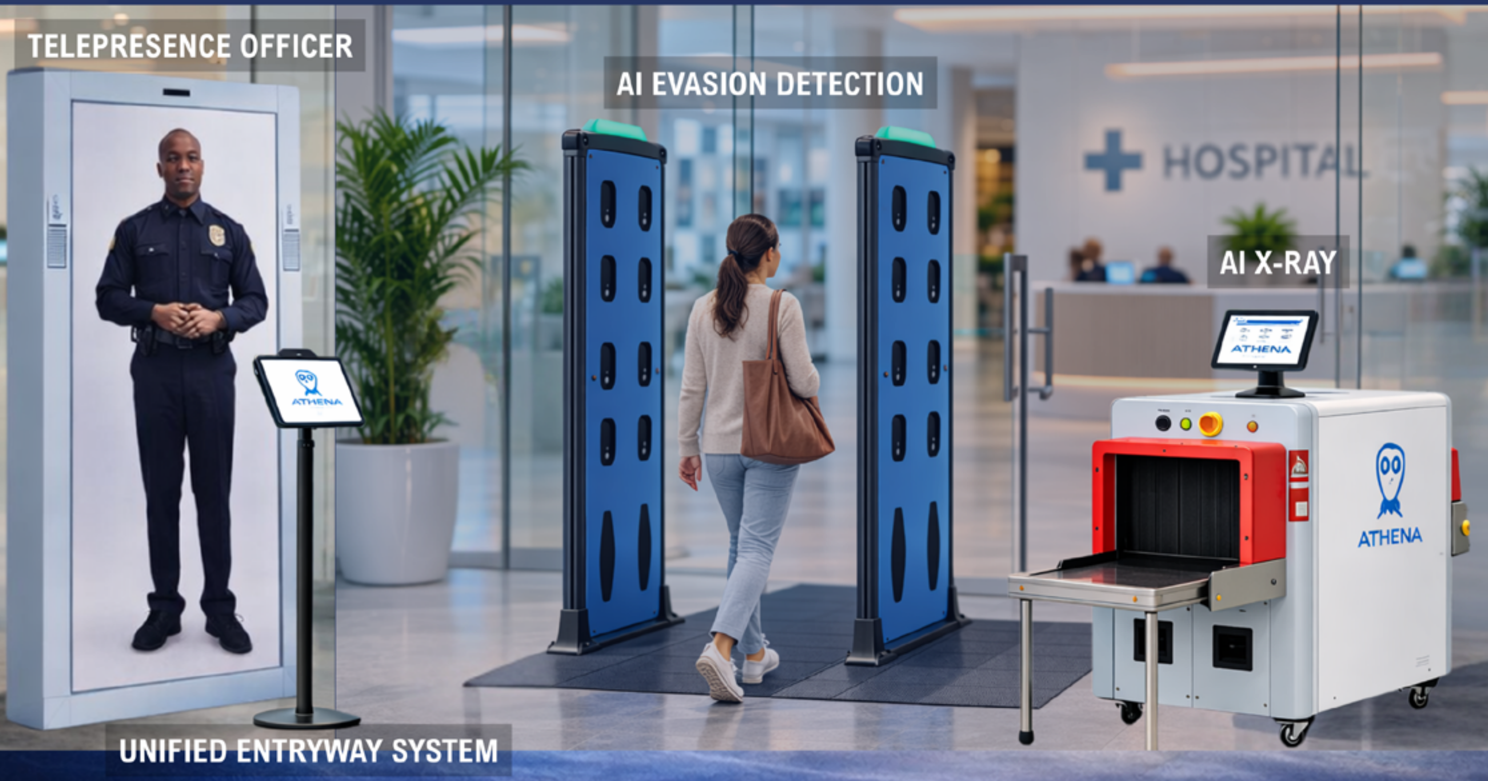
As state safety mandates and workplace violence prevention regulations continue to evolve, organizations are increasingly recognizing that effective security begins before a potential threat enters the building. Facilities that integrate visitor management and weapons detection into a unified entryway strategy are better positioned to protect staff, support compliance, and create safer environments for the people who depend on them every day.

__Chris Ciabarra__ is the Co-founder and CTO/Chief AI Officer of Athena Security.

ATHENA

Reimagine Front Door Security: Unified

Athena Security's unified entryway platform combines **concealed weapons detection**, hospital visitor management, and an **AI X-ray** baggage scanner into **one intelligent system.**



Stop Threats Before They Reach the Lobby

By combining identity verification and weapons screening at the entryway, security teams gain a complete view of who is entering the building and what they may be carrying—before access is granted.

SEE THE SYSTEM IN ACTION

Visit **Athena Security at ISC West — Booth #8140**

Learn more:

www.Athena-Security.com

ATLASIED

COMMUNICATION PLATFROM FEATURES LOUDSPEAKER ENDPOINTS

The IPX mass communication platform features loudspeaker endpoints, visual alerting displays, and the Rapid Alert panic button system, all of which play a crucial role in enhancing security across a range of installations. With a wide variety of form factors suitable for both indoor and outdoor settings, the IPX Series leads the industry, offering best-in-class flexibility, intelligibility, and coverage. *www.atlasied.com/ipx-series-overview*

MARCH NETWORKS

MARCH NETWORKS LONG TERM CLOUD STORAGE

March Networks Long Term Cloud Storage enables secure, scalable video retention without expanding on-premise infrastructure. Using a flexible, tiered model powered by Amazon S3 Glacier, organizations can archive video for years at up to 80% lower cost while keeping recent footage on-premise for fast access. *www.marchnetworks.com/cloudstorage*

HIRSCH

SINGLE INTUITIVE COMMAND CENTER FOR COMPLEX ENVIRONMENTS

Velocity Central provides a single, intuitive command center for managing complex security environments. It brings together perimeter protection, access control, video intelligence, intrusion detection, and identity into one unified operational view. Designed for mission-critical environments, Velocity Central reduces complexity, accelerates response, and gives security teams real-time situational awareness — all backed by Hirsch's federal-grade reliability. *www.hirschsecure.com/us/en-us/products/unification-integrations/velocity-central*

MILESTONE

THE BACKBONE OF YOUR SECURITY SYSTEM

With XProtect video management software as the backbone of your security systems, you can tailor, scale and simplify your video surveillance – all form one centralized platform. Open-platform flexibility means organizations can build and customize more future-proof security systems. Choose from the market's widest choice of cameras, sensors, and IoT devices; and protect your investment with greater cybersecurity and compliance. *www.milestonesys.com/products/software/xprotect/*

ATHENA SECURITY

ATHENA SECURITY'S UNIFIED ENTRYWAY SYSTEM

Athena's unified entryway integrates concealed weapons detection, hospital visitor management system, and AI-assisted X-ray baggage scanner onto the Apple iPad with integrated alerts and reporting. The system includes real-time Person-of-Interest recognition, evasion detection, and threat location. DHS-compliant with offline functionality and self-healing capabilities, this powerful system enables facilities to identify human and physical threats before they enter. *www.Athena-Security.com*