ELEVATE

ISSUE 3

FALL 2025

DRONES ON THE RISE
See how Axon is leading the charge with the latest technology

PUBLISHER LiveView Technologies

EDITORIAL DIRECTOR Noelle Baldwin

ART DIRECTOR Olivia Knudsen

WRITERS Noelle Baldwin, Dave Baker, Steve Lindsey, Mary Rose McCaffrey, Logan Tanner

COVER ART Abigail White

EDITORIAL BOARD Derek Boggs, Jared Davis, Robin Dich, Michael Lamb, Jared Richardson, Logan Tanner

LEGAL ADVISER John Thomas

ELEVATE

ISSUE 3 — FALL 2025

Agent of Change

Reflecting on Security's Most Transformative Decade

BY
Dave Baker

I was recruited by just one company coming out of graduate school. I remember I nearly talked myself out of the interview. Selling cameras didn't seem like the high-tech future I envisioned. I wanted to be in a deeply technical field, solving complex problems. Cameras felt too basic.

But what I discovered was an industry on the verge of transformation—ripe with potential and driven by emerging technology. Until that point, surveillance was dependent on closed-circuit television architecture. Analog cameras and coaxial cabling were the standard. Even today, remnants of that era are still found in many environments.

But in 2013, the IP (Internet Protocol) inflection point was nearing its end. My first sale was for IP encoders—devices that could ingest analog video over coax and output it as IP, allowing customers to modernize their infrastructure without ripping and replacing everything. These sold like hotcakes, and for good reason: IP unlocked access to standard network infrastructure, allowed for rapid software innovation, and enabled remote access to video feeds from anywhere. No more squinting at grainy footage in a dark server room; now, a customer could identify what vehicle hit the fence post from a browser halfway across the world.

IP was more than a technical upgrade—it was a gateway. It paved the way for the cloud to enter the surveillance conversation. With IP, the head end of a surveillance system could be virtualized. Cloud-based platforms offered infinite scalability, centralized management, and the ability to deploy features and updates at the speed of software.

THE CLOUD ERA: VIRTUALIZED, SCALABLE, AND ALWAYS-ON

Cloud changed the game by making surveillance systems location agnostic, not tethering them to on-premises NVRs and DVRs. With cloud-native or hybrid systems, users could securely manage, access, and share video from anywhere with an internet connection.

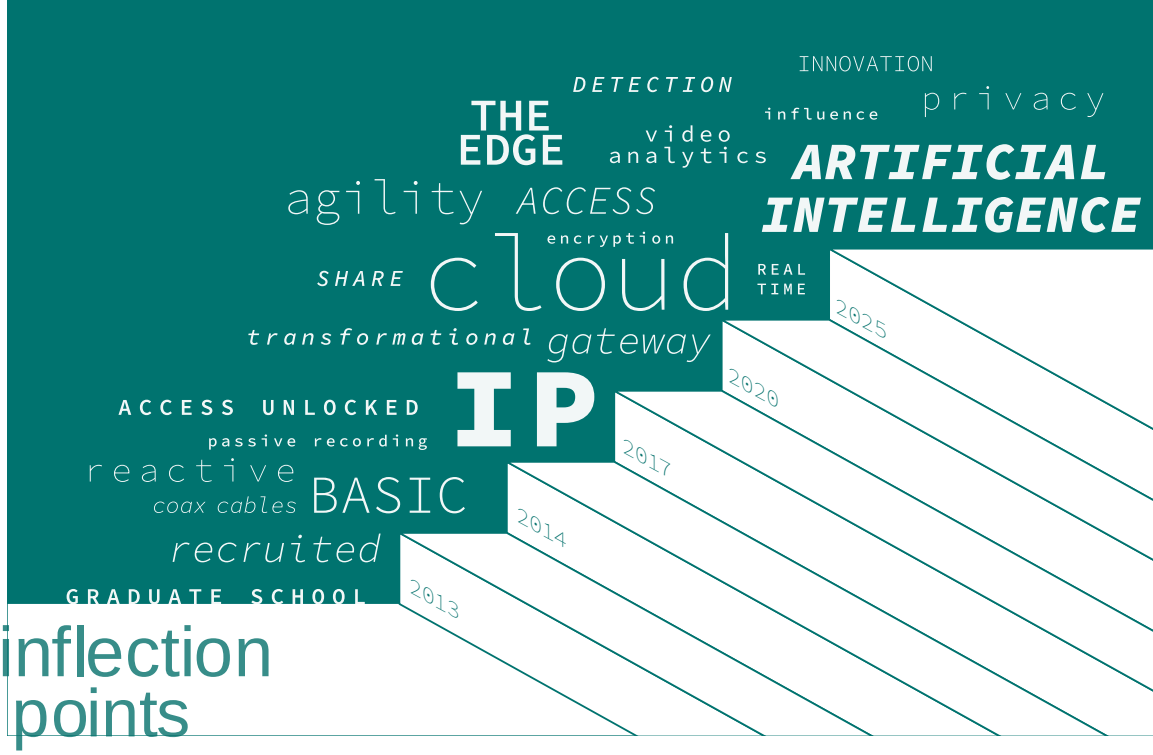
For multi-site enterprises, this was transformational. A retailer with 500 locations no longer needed 500 discrete video systems. Central IT could manage firmware, access controls, device health, and incident response from a single pane of glass. This consolidation didn't just reduce complexity—it enabled entirely new operating models.

The possibilities only expanded with the evolution of application programming interfaces (APIs) and integrations. Cloud-based video management system (VMS) platforms began connecting with access control systems, alarm panels, and even environmental sensors. Video moved from being a reactive evidence tool to a real-time factor of an intelligent, interconnected ecosystem.

Cloud also brought a new level of agility. In the traditional model, deploying a new feature meant updating every appliance across the enterprise. Now, updates could be pushed centrally, continuously, and without downtime. The "VMS" evolved from static software to dynamic service—always improving, always iterating.

But when surveillance lives in the cloud, security of security becomes paramount. Questions around data sovereignty, encryption standards, user authentication, and incident response protocols took center stage. The shift was inevitable—and beneficial. Cloud-first security forced the industry to harden itself, adopting best practices from the broader IT world.

Dave Baker,
Security Solutions Architect,
has been in the security industry since 2013 with an emphasis on surveillance technology. Before joining LVT, he spent time with Axis Communications, Avigilon, and Qumulex. He is an ASIS triple crown (PSP, CPP, PCI) and holds industry certifications in VMS/VSaaS, intelligent video analytics, and camera hardware.



THE RISE OF ANALYTICS

In 2014, the company I worked for acquired a video analytics startup. The goal was to integrate that technology into our existing VMS platform. Once a camera can identify a human or a vehicle in real time, the logic you can apply becomes limitless. You can record only when a person enters the scene. You can trigger alerts, tie into other hardware systems, or run complex automation—all based on actionable data. That simple red box represented a shift from passive recording to intelligent surveillance.

Of course, for any of this to work in real-world, mission-critical environments, the analytics had to be accurate. I insisted on programming analytics myself. If something we sold didn't work, I'd go onsite to troubleshoot it firsthand. Those moments were my true education in intelligent video analytics, teaching me not just how the technology worked, but when and how to position it credibly.

INTELLIGENCE AT THE EDGE MEETS INFINITE COMPUTE

From about 2017 to now, we've hit a compound inflection point. Manufacturers began deploying deep learning-based analytics directly on edge devices, and the cloud started to gain traction. The combination of edge intelligence and cloud computing fundamentally reshaped the surveillance industry.

Today, analytic performance is a key differentiator. Artificial intelligence at the edge allows for lightning-fast event detection and classification without the latency of backhauling video. Cameras can now distinguish between a person and a shadow, a vehicle and a tree branch, even a loiterer versus a passerby.

Simultaneously, cloud-based platforms began ingesting this edge data and enriching it—using powerful algorithms to detect anomalies, run cross-site pattern analysis, or trigger advanced workflows. The edge gives us speed and scale.

We're also seeing the rise of metadata-driven surveillance. Cameras no longer just capture footage—they generate structured data about what's happening in the scene. This metadata fuels search, audit, and automation at a level we once thought impossible. You can now type "white truck with ladder rack" and instantly retrieve relevant clips across hundreds of sites. Or configure a system to alert you only when someone approaches a restricted area, lingers more than 15 seconds, and is wearing a backpack. That's not science fiction—that's now.

FROM REACTIVE TO PROACTIVE: THE NEW ROLE OF SURVEILLANCE

The surveillance industry has traditionally been reactive. A theft occurs, an incident happens, and then we go back and pull the footage. But with intelligent analytics and cloud infrastructure, we're moving toward a proactive insights model.

Instead of just seeing the past, we can now influence the present. A system might automatically trigger lights, speakers, or lockdowns based on behavior analytics. Or notify security staff of a crowd forming at a venue before it becomes a safety hazard. Surveillance is no longer just a camera on a wall—it's a real-time sensor in a broader system of awareness.

This shift has also opened new use cases. Retail uses cameras for dwell time and conversion analytics. Cities use them for traffic optimization. Warehouses use them to ensure safety compliance. Video has become more than security—it's now business intelligence.

LOOKING AHEAD

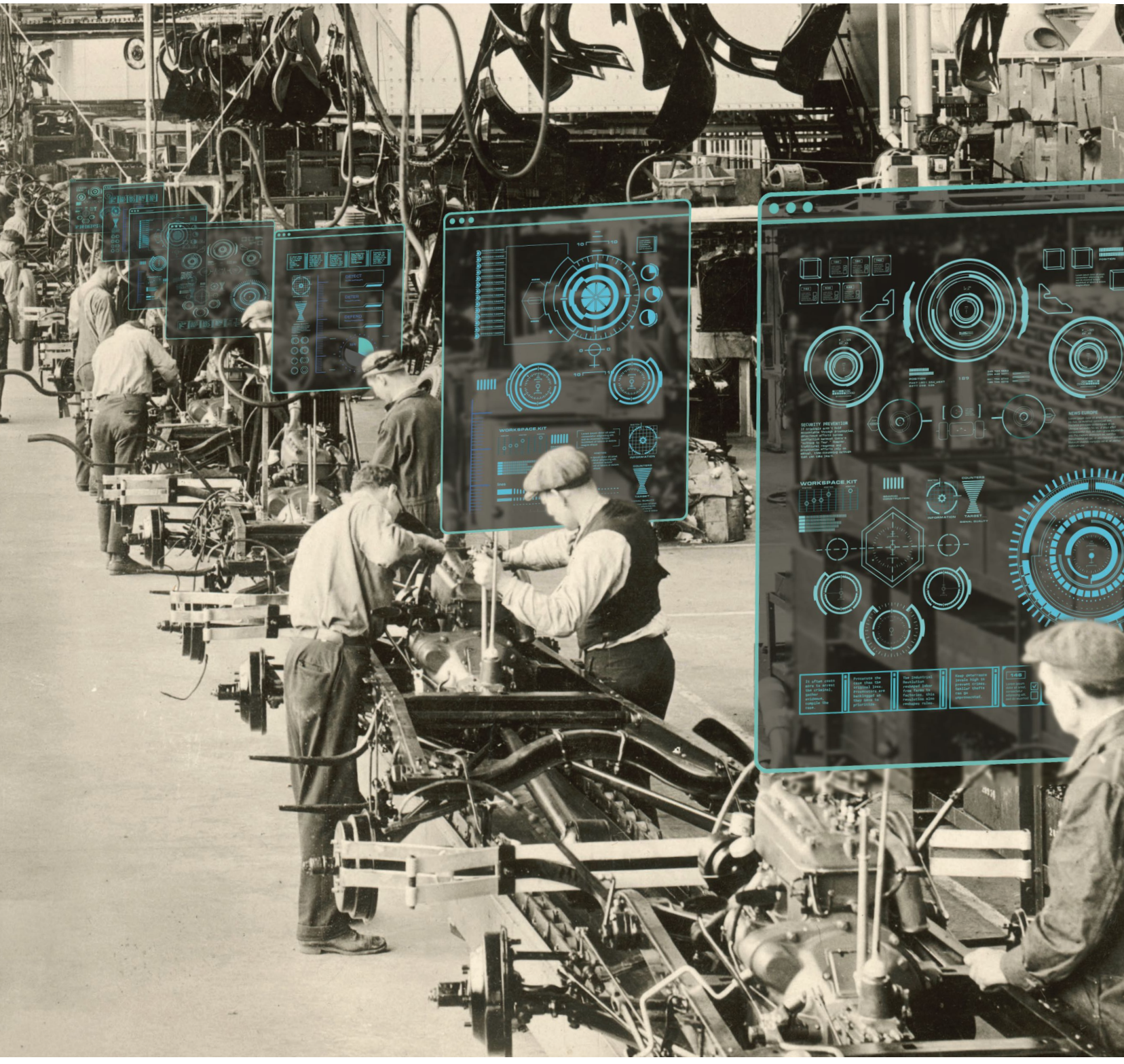
Of course, challenges remain. Accuracy, privacy, and interoperability are ongoing concerns. But innovation moves faster than most expect—and those who embrace the inflection points are the ones who grow with them.

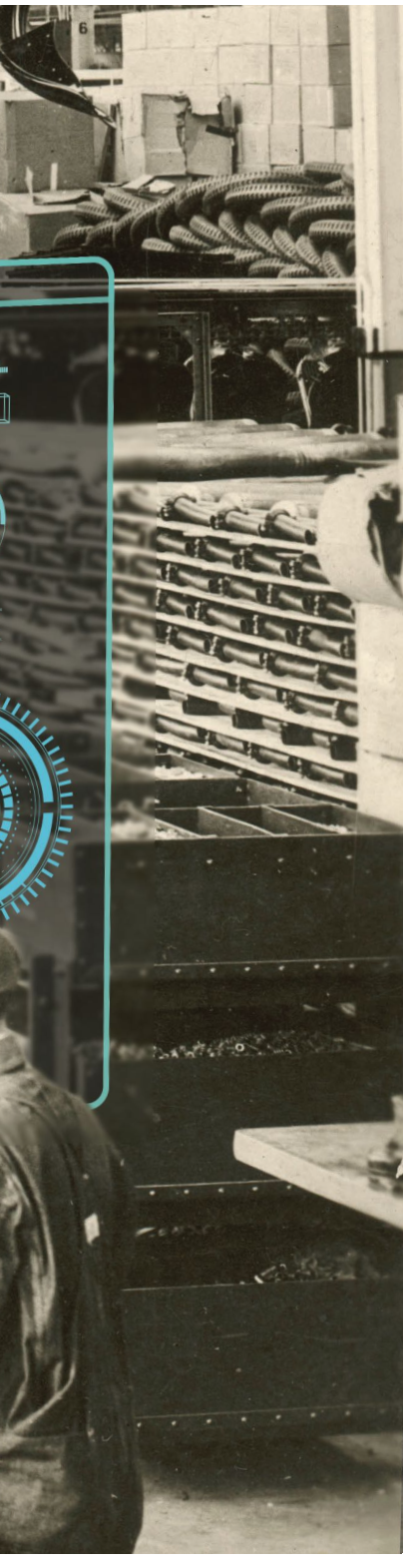
Today, we are equipping cameras with brains, connecting systems across clouds, and layering intelligence atop environments that once relied solely on grainy footage and manual review. The industry is evolving rapidly—and the next decade will likely bring even greater transformation.

From coax cables to cloud orchestration, I've watched this industry reinvent itself again and again. What I thought would be a simple career in cameras turned out to be a front-row seat to one of the most dynamic technology shifts of our time.

SHARE

Read an extended version of Dave Baker's story at **elevate.lvt.com/agentofchange**


WORKSPACE KIT
SECURITY PREVENTION
WORKSPACE KIT
COUNTERS
INFORMATION
TARGET



AUGMENTED IS THE NEW REALITY

How Agentic AI Makes Security Faster, Cheaper, and Far More Efficient

By **STEVE LINDSEY**

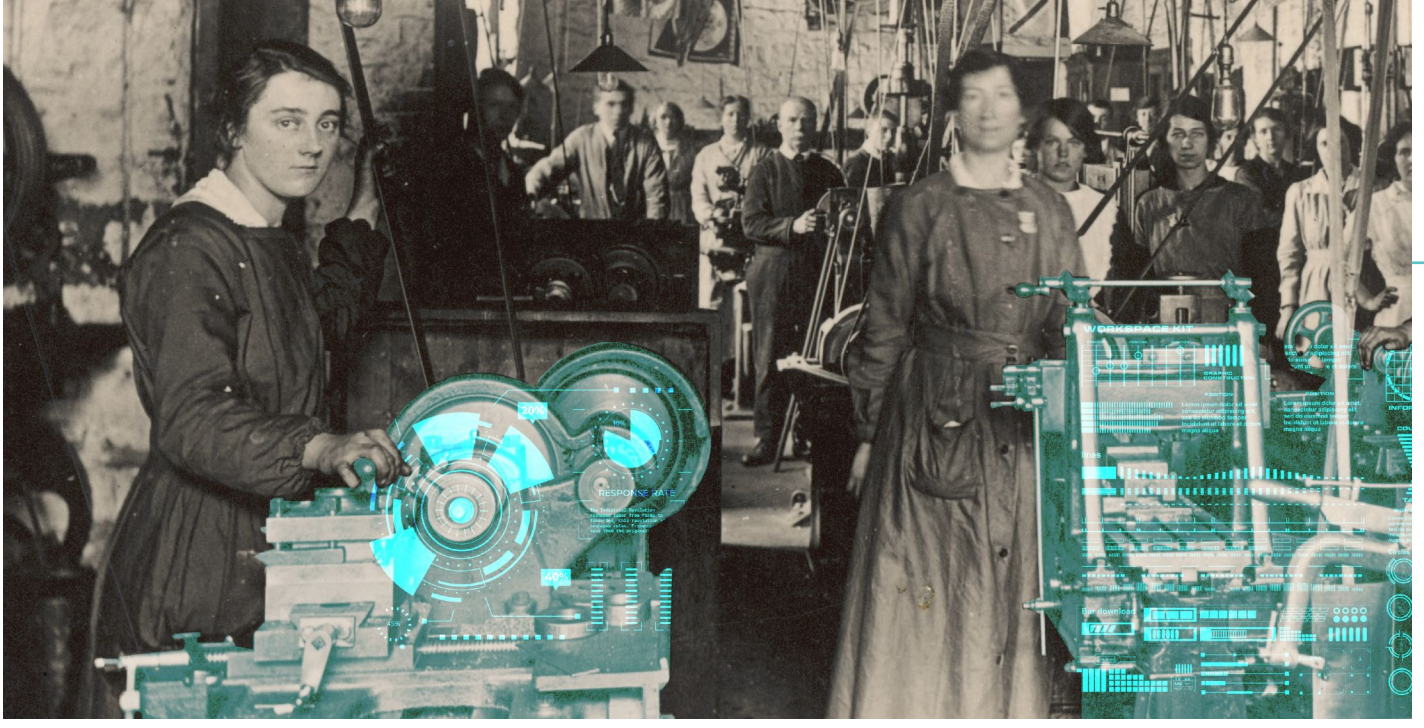
During the Industrial Revolution, an increase in agricultural machinery and decrease in manual labor drove millions to find work in fast-growing cities. In fact, between 1870 and 1910 manufacturing employment rose by more than 8 million jobs.[1] Driving the change was mechanical automation. Inventions like steam-powered engines, the power loom, and electricity soon caused technological unemployment.

It's a theme we've seen throughout history: newer, more efficient machines replacing work once done by hand. And it's happening again. This time in the form of artificial intelligence (AI).

Reports[2] from PwC, McKinsey, and the World Economic Forum estimate 60% of current jobs will require significant adaptation because of AI, and Goldman Sachs predicts 50% of jobs could be fully automated by 2045.

Alarmists say this will put people out of work, but similar to the Industrial Revolution, the AI revolution will just change the work. Just as people shifted from farms to factories, workers will face another generational shift. This time the AI will handle repetitive, menial tasks and free up hours of time for the average worker. Some estimates say AI is already saving workers about an hour a week, but by 2029 that is expected to skyrocket to 12 hours.[3]

The security industry desperately needs a smarter, more effective way to operate, and AI is the answer.



AI in Security

Criminals aren't stopping. In fact, everything from vandalism and violence to panhandling and theft is increasing, which creates unwelcome environments for customers, employees, and communities. Traditionally, companies solve this by hiring more people or adding another single point security solution to their tech stack in an attempt to deter crime. But neither of these are long-term solutions. If the company hires more people, criminals may be deterred for a time, but before long they will find a weak spot to exploit. This leads the company to up the ante again and hire still more security personnel. But security professionals are also faulty because they're human. They experience alert fatigue, need breaks and vacations, and can miss things. And they are expensive. On the other hand, if the company brings on additional security tech, they will need more people to operate it and more people to respond to the alerts the tech generates. But the crutch of this is, either way they are relying on humans to increase deterrence. That is the most expensive and least sustainable way to increase security. It is completely unfeasible to keep hiring more personnel; it leads to a ballooning budget and a fallible workforce.

Security systems today are already good at detecting an intrusion and sending an alert. For example, they're really effective at detecting motion and telling a human that something is moving on the site. This is so common that even simple doorbells on a house can reliably do it. However, the issue is, the security system still relies on a human to respond to the alert and initiate next steps. Reliance on human response is also complicated by alert fatigue, which is where operators are constantly notified by alerts and become desensitized, missing critical alerts and threats.

Steve Lindsey, Chief Information and Technology Officer, was instrumental in designing, forming, and implementing the LVT Platform, the company's video and IoT management system. Lindsey joined LVT in 2011 after leading technology, software, engineering, and development teams at multiple companies including i3 Technologies and Novell. He holds a bachelor's degree in electronic and information technology from Brigham Young University. Outside of all things tech, Lindsey loves mountain biking, music, food, sports, and especially his family. He and his wife Wendy have seven children and live in Utah County.

Agentic AI

This is where agentic AI can step in and make security faster, more efficient, and cheaper. Agentic AI is a type of artificial intelligence that can make decisions and take actions independently to automate multi-step processes, designed to operate more like a human employee. It adapts to different situations rather than being statically programmed. In the example of motion detection, agentic AI not only helps to classify what moved (a human, vehicle, or animal), but also determines the level of threat based on observable context and initiates the next appropriate steps—all without involving a human security guard. Actions agentic AI can take might include turning on spotlights to track the perpetrator or projecting custom messages over the speaker. It can even call out specific features of the intruder, like the color of their clothing, hats, and location on the property. If that still doesn't scare off the intruder, the AI can make the decision to escalate further according to the specifications at that site. That might mean speaking a more imposing message, contacting security, or calling in law enforcement. Essentially, the agentic AI will deal with all of the alerts coming in, manage the ones it can, and only alert guards to problems that need human intervention. It helps remove human error and helps the guards optimize their efforts.

It's a theme we've seen *throughout history:* ***newer, more efficient machines*** *replacing work once done by hand.* ***And it's happening again. This time in the form of*** *artificial intelligence.*

Traditionally, security efforts are divided into jobs to be done—detection, validation, deterrence, response, and prosecution. Prevention (detection, validation, deterrence) is worth its weight in gold over response and prosecution. Obviously, response and prosecution are important. They form a symbiotic relationship with prevention and form a complete security system. And if criminals aren't held accountable through prosecution, deterrence efforts become ineffective because there's "nothing to fear." However, traditional response and prosecution efforts rely on manual, time-consuming methods that can take years. It often costs more to arrest the criminal, gather evidence, compile the case, and prosecute the case than the original loss. Prosecutors are backlogged so they have to prioritize bigger cases. This means smaller thefts can go unprosecuted because it simply isn't worth the time and money.

Agentic AI is the solution to these antiquated practices. It reduces desensitization and increases deterrence through customized messaging, spotlights that pan to detection zones, and other automated responses. Keeping deterrence levels high helps prevent crimes. If AI can help increase effective deterrence, it can help save money in prevention by optimizing human guards and prosecution, which often costs three times more than the initial loss.

Agentic AI also streamlines the evidence gathering process. It removes manual processes so it is easier for investigators to build a case, saving time and resources. Reducing time in turn reduces cost, and less expensive prosecution makes holding criminals accountable easier, which validates the purpose of the security system/efforts to begin with.

The Human Advantage

AI isn't perfect yet and is a long way from completely replacing security personnel. In fact, AI most likely will not replace all security personnel; a human will still need to strategically direct security activities playing the measure/countermeasure game that takes place between the good guys and the bad guys. AI will be really good at taking instructions from humans and performing the work needed to detect those threats and respond to them appropriately. AI excels at work that is monotonous, repetitive, and human-error prone, performing with tireless consistency day-in and day-out.

For example, as bad actors change their tactics, humans will need to be able to research trends and learn the new tactics to better detect and defeat them. AI agents can help humans do the research and find the trends, but ultimately a human has the reasoning, the creativity, and the purpose to strategically plan for a response.

Replacing Humans?

AI is not replacing humans in the security industry. Yet. In fact, I believe we are a long way from that. It will continue to improve as it learns from feedback loops from real-world data. But for now, the right balance of humans and technology can reduce cost, increase speed, and improve accuracy.

Just as the Industrial Revolution reshaped labor from farms to factories, the AI revolution is reshaping roles within industries, including within security. Agentic AI won't lead to technological unemployment but to technological augmentation. It will handle the repetitive, high-volume tasks and reduce human error and alert fatigue, allowing human expertise to show through. Instead of replacing human security guards, agentic AI helps them be more strategic, proactive, and effective. The future of security isn't human or AI but a balance between them that creates safer, more secure environments with a complete security ecosystem.

SOURCES

1. "Employment by Industry, 1910 and 2015." U.S. Bureau of Labor Statistics, U.S. Department of Labor, 3 Mar. 2016, www.bls.gov/opub/ted/2016/employment-by-industry-1910-and-2015.htm.
2. Kelly, Jack. "The Jobs That Will Fall First as AI Takes Over the Workplace." Forbes, 25 Apr. 2025, www.forbes.com/sites/jackkelly/2025/04/25/the-jobs-that-will-fall-first-as-ai-takes-over-the-workplace/.
3. "AI Set to Save Professionals 12 Hours per Week by 2029." Thomson Reuters, 9 July 2024, www.thomsonreuters.com/en/press-releases/2024/july/ai-set-to-save-professionals-12-hours-per-week-by-2029.

SHARE

Know someone who might enjoy this article? Share the online version: **elevate.lvt.com/augmentedreality**

IMAGE COMPOSITES BY OLIVIA J. KNUDSEN, WITH IMAGES BY BY PALERMO89 AND ARCHIVIST/ADOBE STOCK

HOW LEGACY BECOMES LEGEN

Using AI to Enhance Your Existing Security Systems

DARY

BY

Mary Rose McCaffrey

Mary Rose McCaffrey, former CSO Northrop Grumman and Director of CIA Security, is a security expert with over 30 years in government and private industry. She served as Vice President of Security at Northrop Grumman, where she built world-class security and crisis management programs. Previously, she was the CIA's first female Director of Security, holding senior roles across the Intelligence Community, DoD, and NRO. She is a recognized leader in national security and industry collaboration.

Security is a form of risk management, and all security begins with identifying risk. Every company relies on identification risk management as a part of its brand management. The threat is what determines risk. Threats are dynamic. A threat to an individual is different than a threat to an event, an asset, a company, or a military installation. Historically, security programs derive from the threats and risks. Technology has been used in these programs, but current technology continues to help reduce risk.

Security technology has evolved dramatically over the past decades. The purpose of security is to detect and deter, which then better informs the protection of a facility, asset, and/or compound. Security's ability to defend has traditionally relied upon static defense mechanisms with humans taking an action once a camera, alarm, or sensor is notified.

The threat is what determines ***risk.*** *Threats are dynamic.*

Historically, technology advancements have varied in forms. In the early days, that included materials that made an intrusion harder. It evolved with cameras and sensor advancements, which provide faster indicators and warning. The sensors would feed the computer, which relied on an individual to review and act by identifying a potential intruder and addressing the size and scope of the event. Computers got faster and cameras got better, but the lag time between the event and the initial response did not necessarily correspond. Added time frames of response and giving guards post orders were ways to address gaps in the technology, but those tactics did not always solve the problem. Companies traditionally added more labor to security in hopes that would be the sole solution. While it may seem like the logical decision, with today's challenges of different needs and sizes of sites, it's time to consider a force multiplier compound that also includes acreage, fences, sensors, and cameras.

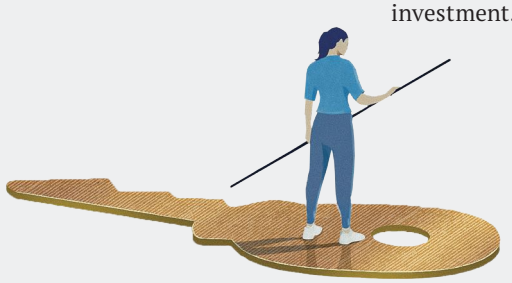
The reality is, over time, equipment ages and humans get complacent. This is manifested when there is a breach, break-in, theft, or attack on an individual or company. Those unfortunate events can be a result of significant gaps in security caused by

ILLUSTRATIONS BY MARCO BACCIOLI

AI is the single technology in the past two years which has the ***potential to transform*** *how security collects and analyzes data.*

the realities of man and machine: broken sensors, intermittent or inoperable cameras, facility features not maintained (parking lot lights, emergency call buttons). After significant security events, there is a great deal of scrutiny, but corrective measures are reactive.

Security is often considered a cost element, so often it ranks lower on the funding priorities. Organizations need to start evaluating security as an enabler to the business, utilizing technology to maximize the resource utility. For example, time and speed to resolution are important in any security event. The speed of an intrusion detection reduces the potential theft, loss, or impact to the business, in turn reducing the impact to the company's costs and brand. The San Francisco Police Department deployed multiple types of security including mobile surveillance units and drones, which enabled not only detection, but also the ability of law enforcement to prosecute offenders. In a commercial vertical, the ability to identify reduces the time an intruder has to try to steal, allowing businesses to reduce loss prevention and contribute to the bottom line. In the federal space, time to detection enables teams to locate and identify intruders and perpetrators while meeting customer response requirements. Technology hardware and software solutions can provide value to current physical security environments. This is an opportunity to posture security as a return on investment.



During my decades leading teams in the federal government and private sector, I watched technology evolve rapidly. It continues to evolve and there is no slowing down. Forensic capabilities married with artificial intelligence can help investigate and close incidents faster. For years, incidents were investigated post-event. Investigators sifted through data, interviewed individuals, and provided a report of the event. This critical information relied on memory of the event by the individual on duty, and hopefully it was captured on a camera in the monitoring center. When it all went smoothly, the investigation could be close to a successful closure, but often there were missing elements. Key investigations may have been closed without knowing all the facts. Criminals, thieves, and adversaries use existing vulnerabilities to their advantage. Security can and should use technology to reduce this gap.

The application of agentic AI provides a capability to identify the intruder(s). Once identified, the options for prosecutorial actions are greater. The camera coverage can discern between a human and a four-legged intruder, perceive the size of a protest, or add visibility to what cannot be seen by the naked eye at night (if employing thermal cameras). Agentic AI has changed the calculus, reducing the gap between

sensing and action. The identification, informing capability buys time. Time enables humans to take appropriate action sooner (i.e., call local law enforcement, deter the bad actor from entering in the first place). Agentic AI can maximize physical security resources and enable the implementation of stronger physical security countermeasures. For example, AI talk down can reduce risk and strengthen your security posture. It independently plays messages warning intruders off the property, intervening without a human guard. This capability can make your company, assets, facilities, or compound a harder target and will convince the threat to go elsewhere.

The reality is, over time, equipment ages and ***humans get complacent.***

As with all technologies, there must be guardrails of utility. One must ask and answer the "who, what, where, how, and when" questions to ensure legality and privacy are not concerns. If there are concerns, what is the planned mitigation? How does the technology address the cybersecurity concerns sufficiently to protect and defend a client's data and personnel? Any technology utility must have a robust cybersecurity posture.

AI is the single technology in the past two years which has the potential to transform how security collects and analyzes data. Let the technology augment the entire security program posture. Customers may be uncomfortable until they understand the rules of engagement, the protections surrounding the data, and how it may relate to their risk management posture. Protection of the backend is as critical as the technology, which gives customers the information to utilize the technology to reduce risk, identify perpetrators, and prosecute as appropriate.

In my roles as a former federal security professional and CSO, new AI-powered security solutions would have provided me with actionable information sooner in protests, construction projects, and other use cases. This is not to say humans and static technologies should be discarded, but having a myriad of solutions allows for optimization of security resources.

Adoption of new technologies takes courage. But courage is bolstered by understanding the benefits of what the technology can provide to augment an existing program or provide a solution to an intractable problem. New security solutions can be easily deployed and adopted. Many are even mobile and can be easily utilized in ways traditional static structures cannot. In addition, the ease of acquisition for all customers allows more flexibility via some annual financial models, allowing security budgets to go further. Also, new technologies can augment guards and help them be more successful. Ultimately, these innovations provide a powerful and flexible means to address modern security challenges more comprehensively than ever before.

SHARE

Share with someone who might enjoy reading this article online: **elevate.lvt.com/legendarylegacy**

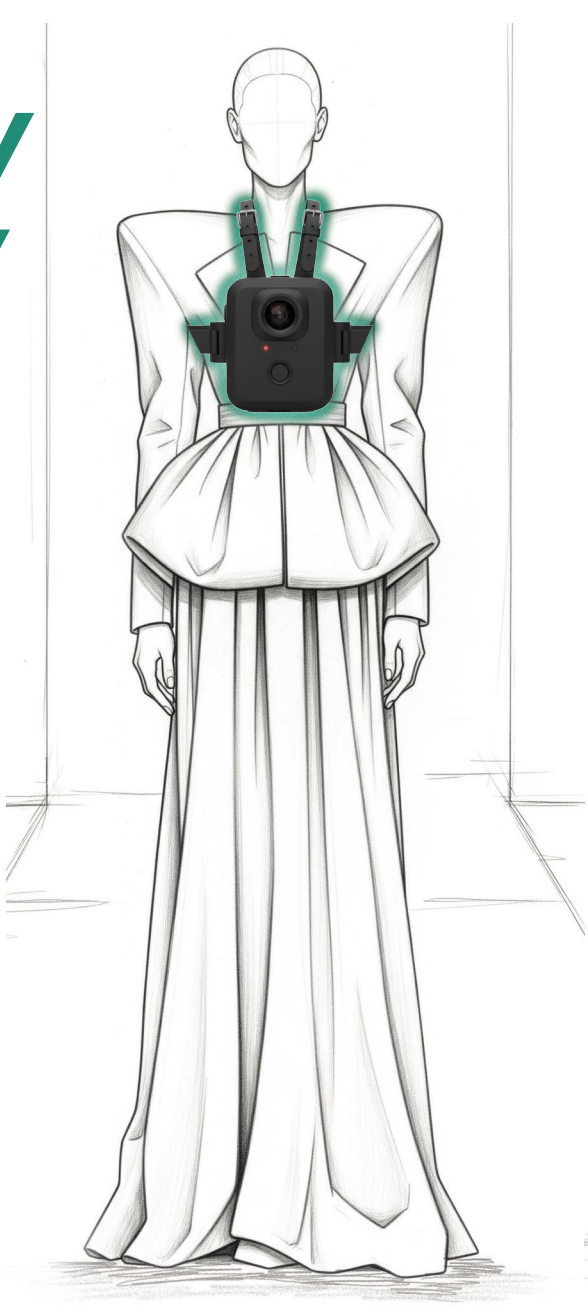
The Security Runway

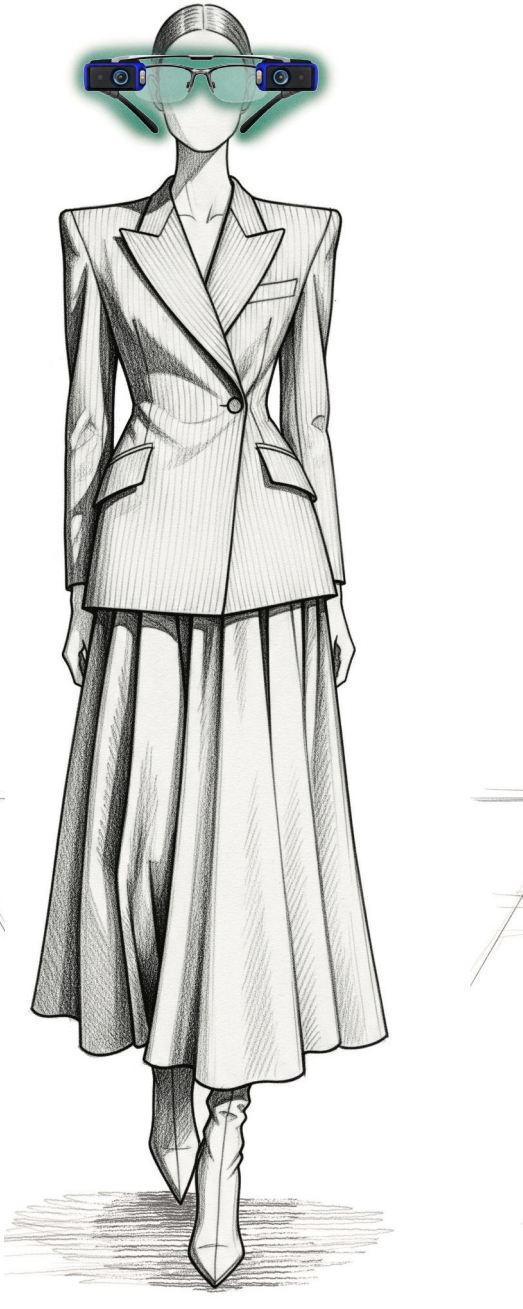
A Fashion Show of Wearable Cameras

BY
Noelle Baldwin and Logan Tanner

Among the fashion faux pas of low-rise jeans and trucker hats, body-worn cameras (BWC) hit the scene in the early 2000s, but didn't become a trend in the U.S. until 2014. In fact, by 2016, about 47% of law enforcement agencies in the U.S. had BWCs in an effort to increase officer and civilian safety as well as decrease liability.

Avant-garde security technology has continued to shrink cameras, increase their capabilities, and make them less cost prohibitive. Eager to get the look and the results, other industries, like retail, began to implement BWCs as part of their security lookbook.



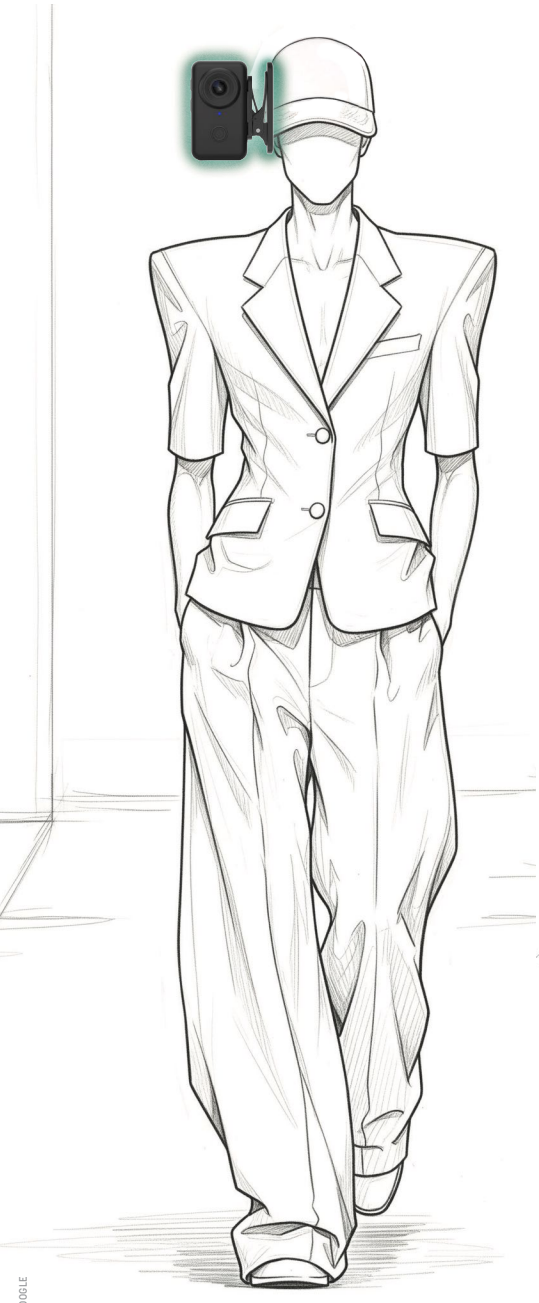


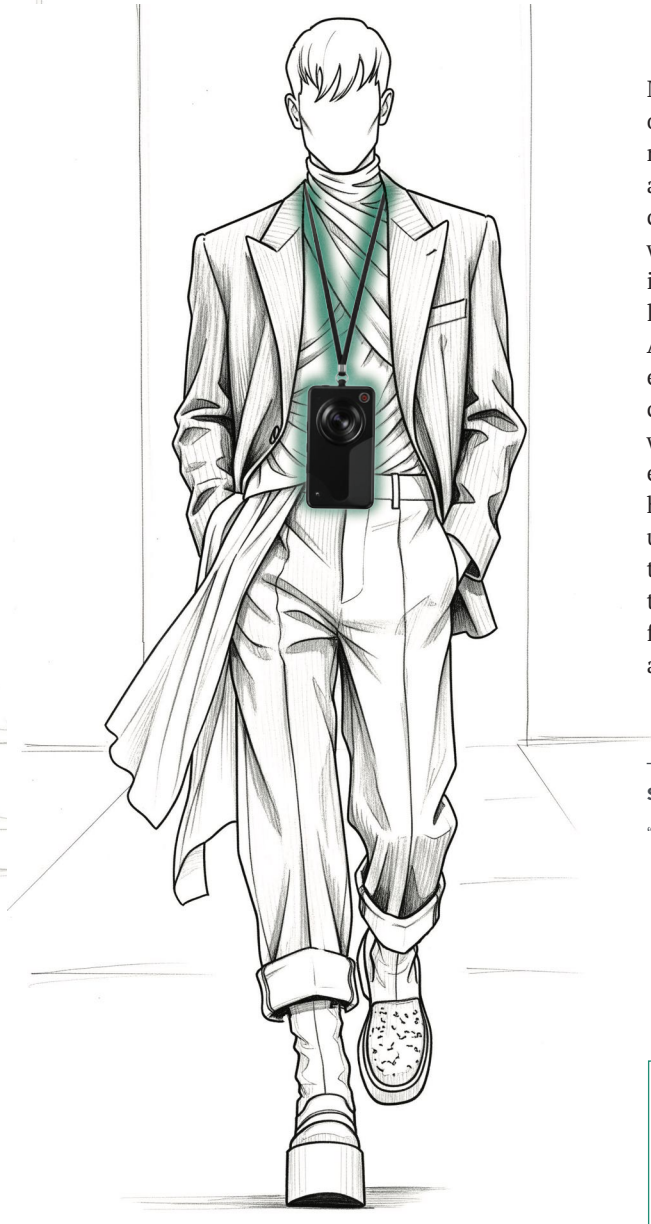
Chest-Worn Cameras:

Long considered a security staple, BWCs return for Fall/Winter 2025. Best worn on the chest, these BWCs often feature impactful extras like extended battery, AI, smart alerts, and wide-angle lenses. The BWC pairs exceptionally well with other timeless pieces like lapel, hat, or spectacle cameras.

Glasses Cameras:

The ultimate in first-person haute couture, camera glasses bring a fresh perspective to the often drab and dowdy world of security. Small but mighty, these stylish focal pieces deliver an unrivaled view for those who demand to see and be seen. Wear as specialty glasses or as a clip-on accessory for any pair of frames for an accentuated look.





Many BWCs now pair smartly with other security staples, offering real-time alerts, AI translation, and more. Security outfits aren't complete until they are adorned with the appropriate BWC to increase accountability, decrease liability, and enhance evidence. And they aren't just for law enforcement and security officers. Retail associates, healthcare workers, construction workers, events managers, and beyond have been seen accessorizing their uniforms with BWCs. And just like that, security has gone from drab to fab, with BWCs as the essential flourish to create a safer and more accountable environment.

SOURCE

"Police Body Cameras." Axon, n.d., www.axon.com/resources/police-body-cameras. Accessed 29 Aug. 2025.

SHARE

If you enjoyed this article, be sure to share it online: **elevate.lvt.com/fashionshow**

Hat Cameras:

This season, hat cameras are back as a beacon of status and style—a hands-free essential for security professionals on the move. Offering a flawless and unobstructed view when clipped to a helmet or headpiece, the hat camera stands as a practical yet bold choice for today's security trendsetters.

Lanyard Cameras:

Too often regarded as a mere accent piece or accessory, the modern lanyard camera has now established itself as a "must have" for security professionals and everyday employees alike. Its simple yet elevated design promises to de-escalate even the most garish offenders while capturing stunning detail. This strong piece can stand alone or pair well with other cameras and looks.

IMAGE COMPOSITES BY OLIVIA J. KNUDSEN, WITH IMAGES GENERATED BY GEMINI, GOOGLE

DRONES ON THE RISE

What Eyes in the Sky Mean for Boots on the Ground

BY
Noelle Baldwin

What was once science fiction is now a reality. Advanced security tools are no longer reserved for blockbuster spies on the big screen. That technology is now real-world ready—accessible to law enforcement, businesses, and security teams to help protect life, secure assets, and deter crime. Axon, a company dedicated to protecting life through innovation, is leading the charge.

Founded on TASER energy devices and later introducing body-worn cameras, Axon's mission is to protect life by equipping law enforcement, prosecutors, businesses, and beyond with tools to enhance safety and accountability.

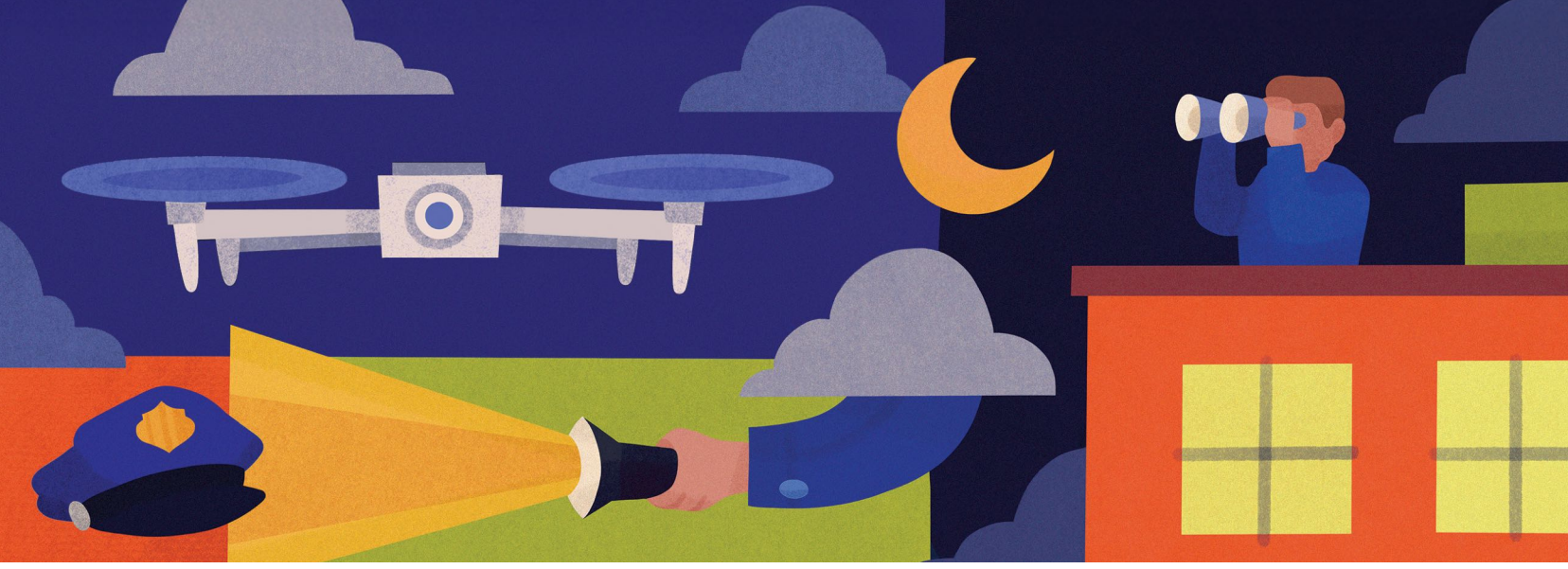
During the COVID-19 pandemic, Axon found that enterprises were facing an increasingly complex security landscape marked by rising threats and limited resources. Security incidents like workplace violence and customer confrontations became more frequent. At that time, Axon officially kicked off its enterprise efforts—offering its ecosystem to businesses outside of law enforcement with security needs.

"Criminal organizations are more emboldened than ever," said Mike Shore, SVP and GM of Enterprise at Axon. "They can inflict real harm with minimal effort. Security leaders are being asked to protect more with less—and technology is how they're doing it."

Today, security leaders find that the old playbooks are no longer enough. Budgets are tight and the traditional model of fixed cameras and patrols can't keep up with evolving threats that are mobile, unpredictable, and often low-cost. They need force multipliers—tools that extend the reach of their teams without a proportional increase in cost or risk. One new solution—drones.

Drones are evolving from a futuristic novelty to a critical component of modern security. They can protect life and improve security at a cheaper price. Drones offer real-time visibility, faster responses, and operational efficiency—at a fraction of the cost of traditional infrastructure. But to truly understand the impact drones have on modern law enforcement and organizations outside of public safety, Axon believes they should be viewed as part of a security ecosystem.

ILLUSTRATIONS BY ABIGAIL WHITE



The Security Ecosystem

Modern security depends on an integrated ecosystem of tools—sensors, cameras, drones, and more. "Drones are highly mobile, intelligent sensors that integrate with CCTV, body-worn cameras, and alarms," said Shore. They can be deployed instantly to provide a unique perspective, and in some cases, they do it quicker, better, and cheaper than other security options.

Axon Air, powered by Skydio hardware, provides real-time aerial support during incidents. With AI-powered autonomous flight and seamless integration into Axon's real-time crime center platform Axon Fusus, it delivers instant visibility into blind spots and live situational awareness to command centers. A second use case is quickly gaining traction: Drones aren't just for responding to incidents—they're being used for proactive patrols. Like a security guard making rounds, they conduct regular surveillance to deter threats and detect issues before they escalate.

For example, unlike traditional CCTV or fixed cameras, drones can give better visuals anywhere on the property. Instead of paying to install power and communication infrastructure for cameras across a large site, a drone can patrol the area for a fraction of the cost. Drones can also replace perimeter patrols, offering superior aerial views that ground-based guards cannot match. "Drones can respond faster and safer without putting people at risk. What we're also finding in enterprise is, drones have a strong ROI beyond security," said Shore.

The same drone that patrols a facility at night can be used during the day for workplace health and safety checks and maintenance tasks—inspecting rooftops, fence lines, and infrastructure. This grants access to hard-to-reach areas and mitigates risk without putting employees in harm's way.

As security needs evolve, organizations are considering threats from both ground and air. The skies are now crowded with millions of commercial and recreational drones. In 2024 alone, Dedrone, the global leader in airspace security, logged 1.2 million illegal drone flights across the U.S., making it clear airspace safety is no longer theoretical—it's a daily challenge.

To help address this for public safety and organizations, Axon acquired Dedrone, which adds another layer of security by detecting, tracking, and identifying unauthorized drones and locating the pilot. It protects over 955 sites worldwide, from airports and stadiums to government and private infrastructure.

The New First Responder

In public safety, when a crisis does occur, drones can become the new first responder (also known as drone as first responder or DFR), providing real-time intelligence to officers before they enter a potentially dangerous situation. For example, when a crime is happening, law enforcement can deploy a drone to have eyes on the situation in minutes. It helps them assess what's happening in real time, know who and what is being threatened, and understand where they need to deploy officers. They can be better prepared to stop the criminal while mitigating the risk to themselves and potential bystanders before setting foot at the scene.

Drones have supported responses to kidnappings, bank robberies, riots, and smash-and-grab incidents. "There was a smash and grab in a major city," said Shore. "And the police department launched a drone in under 90 seconds and just followed the criminals the whole time. They achieved significantly better results at a much lower cost—all while seamlessly integrating with the Axon platform." In another instance, a public safety agency deployed DFR from a dock, successfully tracking some of the suspects in a retail crime incident, making arrests and recovering most of the stolen merchandise.

In the past year, the regulatory environment has evolved significantly, expanding opportunities for drones to operate beyond visual line of sight (BVLOS), largely enabled by a

growing number of FAA waivers. Additionally, executive orders issued in June 2025 have provided clearer guidance for agencies seeking to integrate commercial drones into their operations. However, this future depends on secure, American-made, NDAA-compliant systems. "One of the biggest hurdles to broader drone adoption has been navigating the regulatory landscape. But with these recent changes, we finally have a defined path for deploying American-made drones at scale," said Shore.

Cities across the country are using drones to help their police departments. As of 2023, more than 1,400 agencies deploy drones, and as regulations ease, usage is expected to accelerate.[1]

For businesses, drones are proving to be a powerful tool in mitigating their unique risks. By providing aerial visibility, they help security teams make faster, smarter decisions, often before deploying personnel on the ground. From enhancing employee safety and protecting assets to ensuring compliance and lowering operational costs, drones and drone detection capabilities are enabling organizations to strengthen their security posture without overextending their resources.

> ***"Drones can respond faster and safer without putting people at risk. What we're also finding in enterprise is, drones have a strong ROI beyond security."***
>
> ***— Mike Shore***
> *SVP and GM of Enterprise at Axon*

Ethical Use

As with any technology, drones need rules to ensure their ethical use. Their unique aerial perspective raises important questions about privacy and surveillance. It's why companies like Axon lead with a strong ethical framework rooted in four principles: human-centric, principled, collaborative, and accountable to guide every aspect of their technology.

HUMAN-CENTRIC

"We want tools to extend human capabilities, not replace them," said Shore. Security tools, like drones, are designed to provide security personnel with better information and situational awareness, allowing them to make safer, more effective decisions without putting themselves at risk.

PRINCIPLED

Innovation must protect life, solve crimes, and help businesses but must still strictly comply with privacy regulations. This means that any new tool is designed to be a force for good and is developed with legal and ethical guardrails in place.

COLLABORATIVE

Solutions are built in partnership with law enforcement, business owners, and community members. "The truth is everyone is stretched thin—law enforcement and businesses. But technology can bridge that gap," said Shore. By working together, businesses and communities can create a more cohesive and comprehensive approach to public safety.

ACCOUNTABLE

Axon has a strict documentation trail so everything can be audited. They make sure they can see what happened and why. They ensure transparency and allow for a clear review of actions so they can guarantee that the technology is used ethically and responsibly at all times. This also allows Axon to confirm that all regulations are being met and to adapt when they change.

The Future is Now

The era of drones in security isn't some distant vision—it's happening right now. They are on a trajectory to become a crucial part of public safety and business' security solutions, alongside CCTV cameras. Beyond public safety, drones are a versatile and cost-effective tool that any organization can use to protect people, safeguard assets, and manage risk in an increasingly complex world. "Drones are here to stay," said Shore. "They're being adopted by the Fortune 50, Fortune 200, and Fortune 500. They represent the newest hearing, seeing, and thinking nodes in the modern security ecosystem."

SOURCE

1. "Police Drones: The Complete Guide." Axon, 15 Dec. 2023, www.axon.com/resources/police-drones.

SHARE

Share the online version of this article at: **elevate.lvt.com/dronesrising**

Creating Harmony from Discord

Gain Maximum Efficiency with Orchestration

BY
Noelle Baldwin

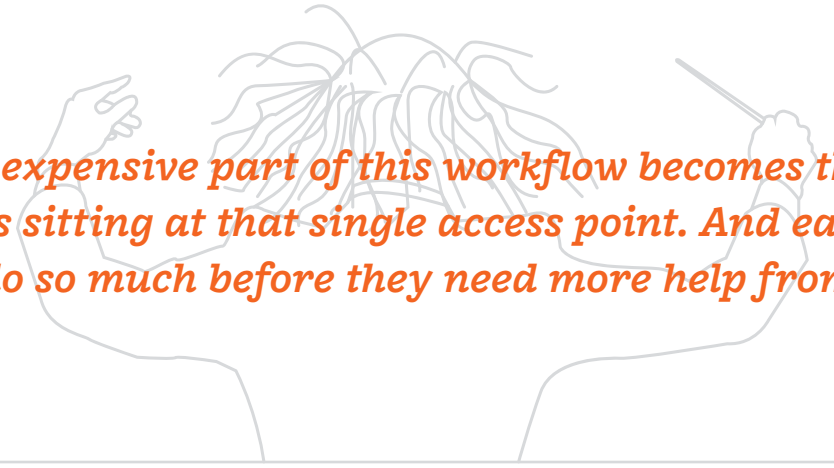
There are dozens of solutions providers that help reduce theft, increase security, and decrease crimes. Some methods include locking shopping carts, security tags, or simple motion detection systems. To simplify the process for their security teams, end users of all this technology pull it into one point, one room, or computer. The problem with this strategy is you still need people to watch and manage that single point. It is not scalable because even though the information is coming to a single point, how do you decide how many people you need to manage, process, and act on that incoming information?

The challenge with this solution is it will continue to compound as you add more technology. Every piece of technology you add to that single access point requires more workers to use it and derive any benefit from it. The most expensive part of this workflow becomes the person or persons sitting at that single access point. And each person can only do so much before they need more help from another. This is an expensive way to secure your property.

For example, say you have cameras, sensors, and an alarm system all sending information to a single computer. All alerts are viewed on that screen by your guard. Anytime an alert is triggered, that guard has to go through their standard operating procedures before any action can be taken, whether that is sending a patrol or calling local law enforcement. That human guard is the bottleneck. They can't act until they process all of the information from all of the inputs.

But what if there were another way to expand your security efforts to not only make it more scalable but also increase its efficiency?

Meet orchestration.



The most expensive part of this workflow becomes the person or persons sitting at that single access point. And each person can only do so much before they need more help from another.

What is Orchestration?

Orchestration is the automated configuration, management, and coordination of computer systems, applications, and services. It helps manage complex tasks and workflows. The goal of orchestration is getting the technologies to work together without needing human input. It will amplify the humans you already have in the chair and help them detect threats more accurately without increasing the number of people you need to manage it.

Security Meets Orchestration

Security systems are currently full of silos—single systems that work on their own. In 2023, the physical security market was valued at $117.7 billion[1] and is expected to nearly double to $211.7 billion by 2030. Also, the Bureau of Labor Statistics[2] states that there are more than 1.4 million jobs in security and protective services with the expectation that it will continue to grow. The numbers speak for themselves—the industry isn't slowing down, and new products and services are offered daily.

Each service or product may fill an important gap in security offerings, but each camera or access control system you add to your security infrastructure is a new independent system for your employees to juggle. Each component is functioning on its own instead of building off of each other to form a cohesive whole. Legacy systems add another layer of complexity to the issue.

For example, you have a system of cameras set up around your buildings but now you are being asked to increase security and need to add access control systems for employees. The cameras function on an entirely separate system than the access control and now instead of your teams monitoring one station, they have to monitor two. Then you are asked to secure the parking lot with mobile surveillance systems. These systems have their own video management system (VMS) that doesn't integrate with your other camera system. Now your team has three systems to monitor. Instead of making their jobs easier, it ends up giving teams more work, which can be especially hard with limited personnel and budget. Also, because the systems function independently, things can be missed, and criminals can slip through your defenses.

Mike Lamb, a renowned loss prevention and asset protection expert with more than 40 years of experience, says it is vital for security systems to start working together. He spent his career trying to increase safety and security while maintaining a pleasant shopping experience for honest customers. This included working for Walmart, The Home Depot, Kroger, and others. Often, said Lamb, companies have dozens of solutions that are trying to solve theft, shrink, and other issues. But they have two main issues—they don't understand their problem and don't have the right equipment to solve their problem.

"Some companies have AP/LP teams that utilize tech and all too often it becomes a launch and leave scenario," said Lamb. "AP/LP teams perhaps have a great idea, stand up the solution, and never truly monetize the value or see the value from the solution."

Which is where orchestration can help. True orchestration isn't

just one system or one solution. True orchestration is business logic. It is all of your solutions working together to create more of a "force multiplier" effect in terms of value.

"Orchestration helps everyone win," said Lamb. "The solution providers grow their business and it's a force multiplier for their clients."

What's the Hold Up?

Why don't different solutions already work together? One reason is coding or the language the solution speaks. Currently, each system uses its own, often proprietary way of speaking. Essentially, it's as if one were speaking Japanese while the other system is trying to communicate in Greek. They are completely different and use different alphabets. The only thing they have in common is that they are both languages. That is how it is with computer code—each is using its own language that doesn't cross over to another system. The machines have got to be able to talk to each other. They've got to be able to make decisions together. And they've got to be able to take action on their own without requiring a human to be involved. That's the only way that these can be effective systems.

Augmenting Security, Law Enforcement, and Prosecutors

According to Lamb, orchestration of security systems is the answer to helping security teams not only be more efficient, but also to increase safety and security without scaring away customers. "Customers are looking for convenience and they vote with their wallet," said Lamb. Currently, businesses are coping with increased theft by placing merchandise behind locks. "They don't want to wait for an associate to unlock the laundry detergent or razors. If that trend continues, it will arguably only grow e-commerce," said Lamb. "Orchestration can help security teams plan a strategy on 'trust but verify' instead of punishing honest customers for the 3–5% which are bad actors."

A good example is computer vision systems that track behaviors (i.e. pacing, biometrics, erratic behaviors, etc.) that can alert teams to potential threats. These systems work together with in-store cameras, body cameras, and store personnel to mitigate against theft and safety liabilities. "It's not just the value of one solution, it's the power of multiple solutions," said Lamb.

Lamb also sees orchestration as a way to help businesses coordinate with law enforcement, district attorneys, and more. "It can help build a case for law enforcement and district attorneys and serve to galvanize those relationships. Instead of data from multiple inputs at multiple locations, businesses can deliver conglomerated data and can even work with other businesses to link criminals to multiple crimes." From start to finish, the harmonization of security tools helps law enforcement find and arrest criminals and gives prosecutors a complete case against them.

What's Next?

Lamb sees a shift coming. "Solution providers are seeing the increase in value proposition if they use orchestration," he said. Security orchestration will help businesses enhance their security posture without increasing staff and workload. It will transform security from a reactive, human-dependent bottleneck into a proactive, scalable, and efficient defense.

SOURCES

1. "Physical Security Market Size, Share | Industry Trends [2032]." Fortune Business Insights, 7 July 2025, www.fortunebusinessinsights.com/physical-security-market-108781.
2. "Field of Degree: Security and Protective Service." U.S. Bureau of Labor Statistics, 29 Aug. 2024, www.bls.gov/ooh/field-of-degree/security-and-protective-service/security-and-protective-service-field-of-degree.htm. Accessed 29 Aug. 2025.

SHARE

View and share online: **elevate.lvt.com/harmony**

IMAGE COMPOSITES BY OLIVIA J. KNUDSEN WITH IMAGES BY TOMASZ RZYMKIEWICZ AND A7880S/ADOBE STOCK

ELEVATE.LVT.COM

LIVEVIEW TECHNOLOGIES

802 E 1050 S, STE 300
AMERICAN FORK, UT 84003

READ MORE ONLINE AT

ELEVATE.LVT.COM