TECHNOLOGY Insights

Fall 2025

Volume 13, Number 2

Computer Vision Quest

AI is making cameras smart, business enablers

Page 18

Early Start

Security should be built in from the beginning

Page 10

Combining Forces

Humans will be empowered by AI, not replaced by it

Page 50

Bilingual Benefits

Practitioners must learn to speak the C-suite language

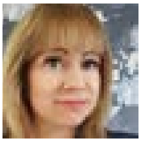
Page 60

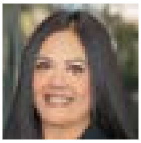
Verified. Bench Tested.
Proven. Compliant. Trusted.

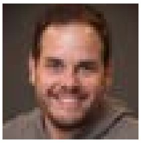
TECHNOLOGY insights

Fall 2025

Volume 13, Number 2







SIA Technology Insights is published twice a year, in the spring and fall, by the Security Industry Association in Silver Spring, Md.

All editions are available at no charge at www.securityindustry.org/techinsights.

Questions, comments and article proposals may be submitted to the editor, Ron Hawkins, at rhawkins@securityindustry.org.

Better Together

Edge AI and agentic AI combine to provide speed and judgment

A recent comment from a senior security leader (formerly with a Fortune 50 company) cut to the heart of a growing debate. He said that edge AI sometimes feels like a pricing tactic, a way for manufacturers to justify higher costs or lock buyers into proprietary ecosystems. While his caution has merit, it risks overlooking edge AI's proven value.

Edge AI has delivered significant advances in physical security, including local video processing, reduced latency, bandwidth efficiency, and faster detection. Many edge AI systems have already proven their worth by providing immediate deterrence through automated warnings, visual alerts, and rapid threat detection. These capabilities have transformed security operations across countless deployments.

Yet even the most advanced edge AI systems face challenges when threats require escalation.

David Marsh (david.marsh@radsecurity.com) is the Vice President of Marketing for Robotic Assistance Devices (www.radsecurity.com).

WHAT EDGE AI MISSES

The promise of edge AI is speed. When systems detect intrusions locally, they reduce delay and improve efficiency. These benefits are real, but they stop there.

Even edge systems with basic response capabilities like automated warnings or visual deterrents typically follow pre-programmed reactions. They lack the contextual intelligence to adapt their response based on evolving situations or to make complex decisions about escalation.

Many edge-enabled devices simply push alerts into a monitoring queue. That is a start, but it is not a complete incident response. Detection and basic deterrence without intelligent, adaptive escalation leave gaps in threat management.

> WHILE EDGE AI PROVIDES SPEED, AGENTIC AI APPLIES JUDGMENT.

HOW AGENTIC AI FILLS THE GAP

Agentic AI does not just detect, it decides and acts.

While edge AI provides speed, agentic AI applies judgment. It interprets context, evaluates risk, and

> RATHER THAN RESPONDING WITH A SINGLE FIXED BEHAVIOR, AGENTIC AI ORCHESTRATES MULTIPLE ACTIONS BASED ON POLICY, PRIORITY AND EVOLVING CIRCUMSTANCES.

chooses how to respond. This is the difference between automation and intelligence. One triggers a light or alarm. The other takes ownership of the situation.

By embedding agentic AI at the central monitoring station (CMS) operator level, escalation happens instantly, response delays are eliminated, and edge AI's capabilities are fully realized.

COORDINATED, AUTONOMOUS RESPONSE

Many edge systems already offer basic automation. They play a recorded voice message, flash a light, sound an alarm. These measures can deter casual intrusions, but they lack adaptability.

Agentic AI adds an intelligence layer to those actions. It determines whether to escalate,

engages with the subject in real time, notifies stakeholders, and records the entire interaction for reporting. These decisions happen in parallel, not in sequence. That alone creates a significant operational advantage.

Rather than responding with a single fixed behavior, agentic AI orchestrates multiple actions based on policy, priority and evolving circumstances.

Most legacy security systems follow a linear process: detect, review, decide, respond. Each step introduces delay. Agentic AI shortens that cycle by running multiple actions simultaneously. The system detects, speaks, alerts, escalates and records in parallel. That means faster outcomes, fewer missed incidents, and a more proactive posture.

The difference is not just technical. It is operational.

HYBRID ARCHITECTURE, SMARTER SECURITY

The future is not edge versus cloud. It is hybrid.

Edge AI delivers real-time detection and local automation. Agentic AI provides autonomous decision-making and intelligent escalation. Cloud platforms offer logging, coordination and compliance oversight.

This hybrid structure reflects how most sites operate today. Local devices operate independently but trigger higher-level action when needed. Agentic AI acts as the link, making decisions in milliseconds and initiating appropriate responses without relying

> PERIMETER SECURITY IS SHIFTING FROM REACTIVE TO PROACTIVE, WITH LAYERED APPROACHES THAT DETER, DETECT AND DENY.

AGENTIC AI DETERMINES WHETHER TO ESCALATE, ENGAGES WITH THE SUBJECT IN REAL TIME, NOTIFIES STAKEHOLDERS, AND RECORDS THE ENTIRE INTERACTION FOR REPORTING.

on a centralized operator queue.

Perimeter security is shifting from reactive to proactive, with layered approaches that deter, detect and deny. A hybrid approach using edge and agentic layers supports this transition with greater speed and resilience.

REAL-WORLD ADOPTION

Agentic AI is not a concept. It is already in use across monitoring centers, enterprise campuses, and state and local government sites. It integrates with ONVIF-compliant cameras, leading video management system (VMS) platforms, and legacy alarm systems. Monitoring providers use it to increase coverage, verify events automatically, and reduce staffing burdens without compromising accuracy.

Adoption is growing because the results are

clear: faster response, reduced false positives, and more scalable operations.

WHAT TO ASK NOW

As security leaders evaluate new technologies, speed is only one factor. Additional questions include:

- Does it reduce mean time to response?
- Can it handle multiple incidents simultaneously?
- Does it integrate with the existing security stack?
- Will it scale as more devices are added?
- Does it eliminate operational bottlenecks?
- Can it produce return on investment (ROI) through measurable outcomes?

These are the benchmarks for modern physical security. Agentic AI helps to meet them all. ◀

> ADOPTION IS GROWING BECAUSE THE RESULTS ARE CLEAR: FASTER RESPONSE, REDUCED FALSE POSITIVES, AND MORE SCALABLE OPERATIONS.

Integration by Design

Security should fit seamlessly into modern buildings

Paul La Vigne (plavigne@tssbulletproof.com) is Chief Marketing Officer at Total Security Solutions (www.tssbulletproof.com).

As safety concerns rise in public and commercial spaces, a key question emerges: How do you secure a building without making everyone inside feel that they are in danger?

Traditional security measures like reinforced bars, electronic turnstiles, and metal detectors can be jarring. They may provide physical protection, but they fail to offer emotional reassurance or peace of mind. Security professionals and designers are now embracing a new philosophy: Security that is built into the environment, not bolted on afterward.

THE DOWNSIDE OF TRADITIONAL SECURITY MEASURES

Traditional physical security has often been designed around worst-case scenarios, with

> TRADITIONAL SECURITY MEASURES MAY PROVIDE PHYSICAL PROTECTION, BUT THEY FAIL TO OFFER EMOTIONAL REASSURANCE OR PEACE OF MIND.

isolated products added as standalone solutions. But without thoughtful integration, these features can interrupt the purpose of the space, sending the wrong message to the people inside.

Walk into a school with heavy, visibly reinforced doors and you are reminded immediately of the threats they are meant to stop. In a healthcare environment, armored reception barriers can undermine the sense of calm and trust that is critical to care. In both cases, the design conveys the message that something could go wrong, and that can make people, understandably, feel unsafe.

In addition, overly visible or piecemeal solutions – like a camera at the entrance or a lone alarm panel – may give

a false sense of security, especially when basic safety protocols like secure entry vestibules or door management procedures are missing.

True security starts with identifying what people are being protected from. In high-threat environments, where targeted, purposeful attacks with high-caliber weapons are a real possibility, more robust measures are needed. But in many commercial and public settings, the threat is often from individuals who act alone and without advanced tools. Security in these environments should be focused on delaying or deterring a threat.

Barriers that absorb an initial wave of violence can buy the seconds needed for people to react, respond or escape. This level of security lends itself to customized solutions that fit the space and are a part of the building.

SECURITY THAT BELONGS RATHER THAN INTRUDES

Integrated security begins with a mindset shift from bolting on equipment after the fact to including

> INTEGRATED SECURITY BEGINS WITH A MINDSET SHIFT FROM BOLTING ON EQUIPMENT AFTER THE FACT TO INCLUDING PROTECTION IN THE EARLIEST DESIGN CONVERSATIONS.

protection in the earliest design conversations. When done well, security elements blend seamlessly into the surrounding materials and spatial flow.

While catalog products will often look out of place, custom ballistic doors, framing and windows can be manufactured to match the finishes, proportions and aesthetics of a given space. These systems are not hidden, but they are not in your face, either. They simply fit the space.

A school might have a vestibule designed with laminated wood finishes that look no different than any other architectural detail. A healthcare facility could have secure transaction windows built into its reception desk with no visible difference from the adjacent cabinetry. In historically significant

buildings, bullet-resistant features can even be fabricated to preserve the appearance of original woodwork or metalwork.

People move through these spaces without a second thought, but those responsible for safety know the infrastructure is there and is effective.

WHY EARLY COLLABORATION MATTERS

Achieving seamless integration between safety and aesthetics requires early collaboration with architects, contractors and security system manufacturers. This provides clarity about what is possible through a clear understanding of what the physical space can accommodate and how different components might affect traffic flow, code compliance and aesthetics. In addition, it helps to control costs. Changes made late in a project tend to be expensive. With advance planning, manufacturers can often offer creative, more affordable alternatives that still meet performance goals.

WITH ADVANCE PLANNING, MANUFACTURERS CAN OFTEN OFFER CREATIVE, MORE AFFORDABLE ALTERNATIVES THAT STILL MEET PERFORMANCE GOALS.

Early collaboration also ensures that the right level of protection is chosen. While there are established performance standards in the industry (e.g., UL, ASTM, NIJ), many building owners and design teams are not familiar with them. They may simply say, “We want to protect this building from a shooting.” By working closely with a trusted security partner, though, project teams can assess the threat profile, understand what level of defense is appropriate, and avoid overbuilding, which can drive up costs, add unnecessary weight, and limit design options.

A SMARTER STANDARD FOR SAFER SPACES

The idea is not to trade aesthetics for safety, or vice versa. It is to marry the two through thoughtful planning and customization. When

physical security is designed to blend into its environment, when people cannot see the difference, then they need not *feel* different about it.

Physical security can support the purpose of a space, rather than disrupt it. A secure vestibule does not need to feel cold. A ballistic transaction window does not need to look like a checkpoint. When security is customized to the architecture – using the same materials, proportions and finishes – it becomes a part of the environment, not a warning about it.

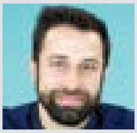
The key is understanding the actual threat profile, applying the right standard, and designing a solution that works for both the people inside the space and the community it serves. ◀

> WHEN SECURITY IS CUSTOMIZED TO THE ARCHITECTURE – USING THE SAME MATERIALS, PROPORTIONS AND FINISHES – IT BECOMES A PART OF THE ENVIRONMENT, NOT A WARNING ABOUT IT.

The Rise of Vision-Enabled Operations

Video data is no longer just about security

Chris Sisto (csisto@solink.com) is the Vice President of Product at Solink (www.solink.com).



For decades, physical security has meant alarms, guards and maybe a wall of CCTV monitors.

Cameras recorded a ton of video, but it was only ever reviewed after an incident, if at all. All those hours of footage were essentially left to waste, regardless of the secrets they had to tell.

But today, security infrastructure is being reimagined as a source of continuous operational insight. Cameras that were once passive recorders are now becoming active sensors in enterprise ecosystems.

This transformation marks the beginning of a new era, unveiling vision-enabled operations. This refers to the use of AI and video intelligence to

THESE SYSTEMS DO NOT JUST SEE, THEY UNDERSTAND CONTEXT AND DETECT ANOMALIES AND SURFACE TRENDS THAT WERE PREVIOUSLY INVISIBLE.

transform everyday video into a source of real-time business insight. These systems do not just see, they understand context and detect anomalies and surface trends that were previously invisible.

Rather than treating video systems as standalone tools for loss prevention or perimeter monitoring, forward-looking organizations are integrating video with operational data to drive improvements in efficiency, compliance, staffing and customer experience. The result is a unified business operation in which video and data infrastructure move in sync with real-time activity across departments and locations.

OLD MODEL: FRAGMENTED AND REACTIVE SYSTEMS

Traditional physical security has relied on hardware-heavy and

THE RESULT IS A UNIFIED BUSINESS OPERATION IN WHICH VIDEO AND DATA INFRASTRUCTURE MOVE IN SYNC WITH REAL-TIME ACTIVITY ACROSS DEPARTMENTS AND LOCATIONS.

siloed tools like motion sensors, door contacts, and DVRs. This add-as-you-go approach fails to scale. It becomes bulky and expensive, opens a wide attack surface for bad actors, and most importantly, lacks any ability to generate actionable insights from the vast amounts of video data being collected.

Focusing too closely on tactical physical security wins can result in massive missed opportunities for operational excellence. Whether identifying bottlenecks on the floor, spotting repeat fraud tactics, or learning from customer behavior, legacy systems simply were not built to capture the full value of what cameras can see.

In an era where data is currency, relying on video without intelligence leaves organizations blind to what is happening in their own environments.

CAMERAS BECOME THE PRIMARY SENSOR

Across industries, businesses are repositioning video infrastructure as a foundational data source. Cameras are one of the most powerful sensors when connected to the right tools. They can fuel insights for loss prevention, operations, security, compliance, finance, HR, IT, and even marketing.

High-definition, cloud-connected cameras are no longer just passive observers. When layered with metadata from access control, point of sale (POS), or Internet of Things (IoT) systems, they become a

powerful platform for insights.

This is the core of vision-enabled operations: Using video cameras as smart sensors and sources of active intelligence, not just a recording tool.

VISION-ENABLED OPERATIONS BEYOND SECURITY

The power of camera-based systems lies in their versatility. While they still play a critical role in theft deterrence and incident review, their reach now spans across departments.

- Operations teams use video to identify inefficiencies, monitor workflows, and optimize staffing based on real-time activity.
- Compliance teams automate audits and ensure policies are followed, reducing in-person checks and reporting time.
- Marketing leaders analyze foot traffic, dwell times, and customer interactions

> IN AN ERA WHERE DATA IS CURRENCY, RELYING ON VIDEO WITHOUT INTELLIGENCE LEAVES ORGANIZATIONS BLIND TO WHAT IS HAPPENING IN THEIR OWN ENVIRONMENTS.

> THIS IS THE CORE OF VISION-ENABLED OPERATIONS: USING VIDEO CAMERAS AS SMART SENSORS AND SOURCES OF ACTIVE INTELLIGENCE, NOT JUST A RECORDING TOOL.

to improve merchandising and campaign performance.

- IT teams benefit from fewer maintenance incidents and faster time to resolution because of remote diagnostics and cloud-managed systems.
- HR and finance teams use video to verify workplace incidents, monitor cash handling, and support shrink prevention.

AI, AUTOMATION AND THE FUTURE OF SECURITY OPERATIONS

As environments grow more connected, cameras are uniquely positioned to act as the digital eyes of the business. The next

evolution will be driven by even more advanced technologies. AI agents will monitor hundreds of feeds for defined events, anomalies or policy violations and take action on incidents like:

- Long service lines causing potential customers to drop-off
- Unauthorized parties breaching the property or loitering in a specified zone
- A sequence of high-risk transactions linked to a specific employee or location
- New in-store merchandising displays changing customer traffic flows
- Vehicles or people on watchlists entering the area

Cross-functional access to video data will enable every department to extract relevant insights without needing a security analyst to interpret it.

The rise of vision-enabled operations means that physical security leaders are no longer just gatekeepers. They are becoming data stewards, enabling faster, smarter decisions across the enterprise. ◀

REAL-WORLD USE CASES

- ▶ Paradies Lagardère is leveraging AI-driven camera analytics to customize airport shopping experiences. By tracking real-time foot traffic and monitoring peak hours, they aim to better understand conversion rates and average revenue per guest, thereby enhancing customer satisfaction and optimizing operations.
- ▶ Yum Brands, the parent company of Taco Bell, Pizza Hut, KFC, and Habit Burger Grill, is integrating AI technologies to enhance their operations. This includes voice-activated order-taking AI to improve drive-thru efficiency and computer vision tools to optimize restaurant workflows through real-time insights.
- ▶ DHL is utilizing AI and computer vision to monitor and analyze movements within their logistics facilities. This technology helps detect issues like speeding, incorrect movements, and parking violations, leading to improved workplace safety and compliance.

Is Your Security Solution Secure?

Endpoint vulnerabilities must be addressed

Six years ago, a receptionist opened an email on her work computer. A seemingly ordinary, pedantic task. Unbeknownst to a menagerie of IT professionals at the time, this message was from her personal web-based email. But, still, none of this was out of the ordinary.

For a plot twist, let us go back six months before she opened the email. A group of hackers had gained access to the municipal active directory for this same environment. While inside the network, they did all the standard things a hacker would do to find the path of exploitation. They even changed the active directory password of the administrator, which they acquired because it was weak and re-used. They created

Ted Nass (ted.nass@avexon.com) is the Co-Owner of Avexon (www.avexon.com).

a new account in the active directory with administrator privileges. They made SQL accounts as well. Then they created a seemingly common looking email to execute chaos and delivered it via personal email, on a work computer, to the nicest of employees.

> WITHIN ABOUT TWO MINUTES OF THIS EMAIL LINK BEING CLICKED, ROUGHLY 4,000 MACHINES WERE COMPROMISED. SCREENS TURNED WHITE, CRAZY MESSAGES APPEARED, SQL DATABASES SHOWED SPIKES IN RESOURCES, AND FIREWALLS WERE ABLAZE.

Within about two minutes of this email link being clicked, roughly 4,000 machines were compromised. Screens turned white, crazy messages appeared, SQL databases showed spikes in resources, and firewalls were ablaze. Comically, in an attempt to stop the chaos, the Internet was quite literally unplugged to stave off more damage.

Unfortunately, it was too late. Servers,

> AN ORGANIZATION DOES NOT NEED TO BE A MASSIVE CORPORATION TO HAVE SECURITY SOLUTIONS DESIGNED TO FIT THE ENDPOINT (PHONE, DESKTOP, SERVER) ENVIRONMENT.

PCs, databases and even backups were all compromised. The organization came to a complete halt, one that would take about a year to recover from.

However, there was no ransom. There was no demand. There was not even a claim of responsibility by any group. Someone did this just for fun.

ENDPOINT SECURITY

Small to medium businesses often have not thought twice about letting employees have access to their personal email, or about allowing users to connect phones to the corporate Wi-Fi.

An organization does not need to be a massive corporation to have security solutions designed to fit the endpoint (phone, desktop, server) environment. Endpoint security is the easiest way to leverage a solution, often

through engagement with a managed service provider (MSP). Even without high-powered, next-generation firewalls or enterprise-level knowledge of switching and routing, anyone from a municipality to a five-person law-firm can get the same level of security that the big names use.

In short, there is no need to tell people that they are no longer allowed to check their personal email at work. (Fun fact: Even organizations that implement such a ban likely allow employees to connect their phones to the company Wi-Fi – where they are still checking personal email.)

DEFENDING AGAINST ATTACKS

If an endpoint security solution had been in place, the hack described at the beginning of this article would have played out very differently. Software would have seen malicious code execution and immediately quarantined the machine from the network. Encryption and decryption keys would have been observed in flight, captured and stopped. An AI-driven security operations center (SOC) would have seen the information come from the endpoint before quarantine, compared it to a list of known exploits, and immediately warned senior leaders of an unfolding attack. This same SOC could also update endpoints with information about recent attacks and exploits suffered by big corporations, allowing the organization to acquire knowledge about preventing similar attacks without having to learn the hard way.

But if you have a next-generation firewall that stops malicious traffic, why

> IS YOUR FIREWALL UPDATED IN REAL TIME, MONITORED BY A SOC, AND UPDATED INSTANTLY WHEN AN ATTACK UNFOLDS AT ANOTHER BUSINESS YOU MAY NOT HAVE EVEN HEARD OF? LIKELY, NO.

worry about an endpoint? Well, is your firewall monitored by a SOC and updated instantly when an attack unfolds at another business you may not have even heard of? Likely, no.

Network segmentation is also key to security. There is no reason the receptionist's machine needs access to the vLAN for cameras, just like there is no reason a guest's phone on your Wi-Fi needs access to the same network your point-of-sale transactions are on.

And a server is no more secure than a desktop. At the end of the day, one is built for up-time and demanding resource allocation, the other for a 40-hour work week. Endpoint security – including observation, reporting and quarantine – plays the same critical role for both.

CONCLUSION

The phrase "Never let a crisis go to waste" has been attributed to various

people. The core point of this phrase, regardless of its origin, is, of course, to leverage a difficult situation to learn, adapt and innovate. But the secret to the phrase lies in what no one ever mentions: It does not have to be *your* crisis.

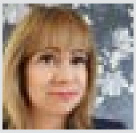
The next time you walk past a coworker and see their personal email open, remember the crisis described above. The next time you give the Wi-Fi password to a stranger, remember that you have no idea what they will do with their phone once connected. The next time you get a pat on the back from a big video management company, ask yourself how long this transactional relationship will last, and whether your interests and needs are being adequately addressed.

And the next time you hear about a big company suffering a network attack, consider how it might have been avoided through the deployment of a solid endpoint solution. ◀

> “
> THE NEXT TIME YOU GIVE THE WI-FI PASSWORD TO A STRANGER, REMEMBER THAT YOU HAVE NO IDEA WHAT THEY WILL DO WITH THEIR PHONE ONCE CONNECTED.

Improving Visibility While Preserving Video Integrity

CNN-based low-light enhancement avoids the pitfalls of generative AI



Jenna Enbuska (jenna.enbuska@visidon.fi) is the Head of Marketing at Visidon (www.visidon.fi).

In the rapidly evolving world of AI-powered imaging, it is easy to conflate all "AI enhancement" with generative methods. But when it comes to critical applications like surveillance, the distinction between generative AI and non-generative, convolutional neural network (CNN)-based enhancement is not just technical, it is fundamental to trust, integrity and evidence reliability.

Surveillance cameras often operate under ultra-low-light conditions, from a few lux down to near-total darkness. In such environments, image sensors struggle. Noise overwhelms the signal, leaving both human vision and automated object detection largely ineffective. Grainy, dark, unclear footage compromises situational awareness and system performance.

CNN-based low-light enhancement addresses this challenge. Unlike generative AI, which generates new data, CNN-based enhancement operates in real time within the camera pipeline as an embedded edge AI solution. It improves both human and machine vision by suppressing noise and boosting object detection accuracy in low-light scenes – without generating new content, such as new pixels.

Generative models, such as generative adversarial networks (GANs) and diffusion models, are designed to fill in missing details by making assumptions about what *could* be present. While powerful in creative imaging, generative approaches raise concerns in surveillance since they may alter details or even introduce new ones that were never captured by the camera.

> “ENHANCING VISIBILITY WITHOUT ALTERING CONTENT ENSURES THAT THE OUTPUT REMAINS A TRUTHFUL REPRESENTATION OF THE RECORDED SCENE, A KEY REQUIREMENT FOR INVESTIGATIVE AND EVIDENTIARY USE.

In contrast, CNN-based enhancement focuses solely on improving the existing signal. Every processed pixel corresponds directly to the input data. The

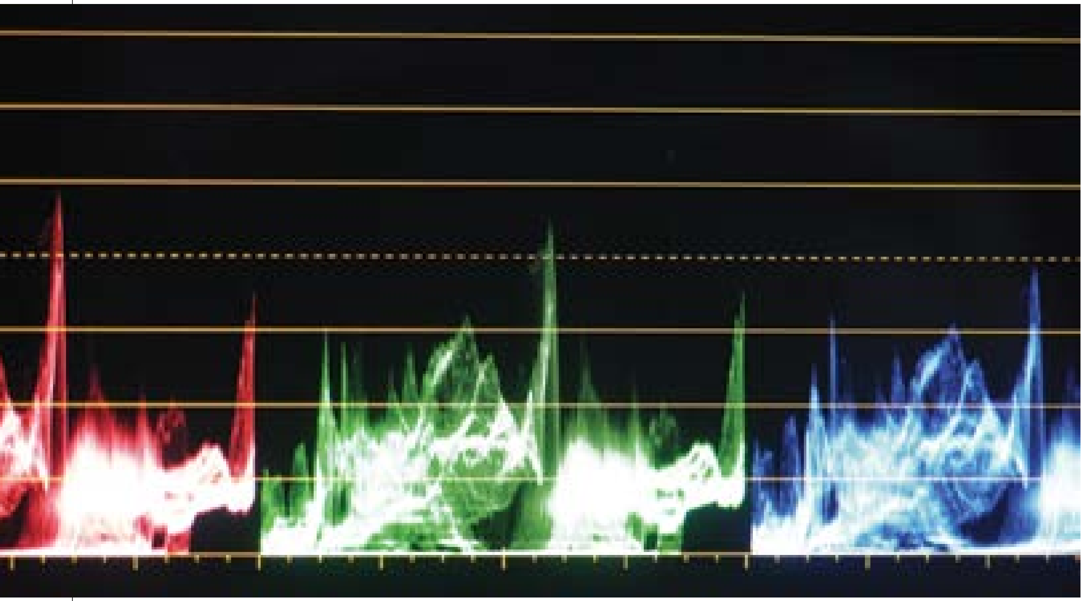
> TRADITIONAL IMAGE SIGNAL PROCESSORS STRUGGLE TO FULLY SEPARATE NOISE FROM SIGNAL, AND AMPLIFYING THE REMAINING SIGNAL ALSO AMPLIFIES NOISE, DEGRADING VISUAL IMAGE QUALITY.

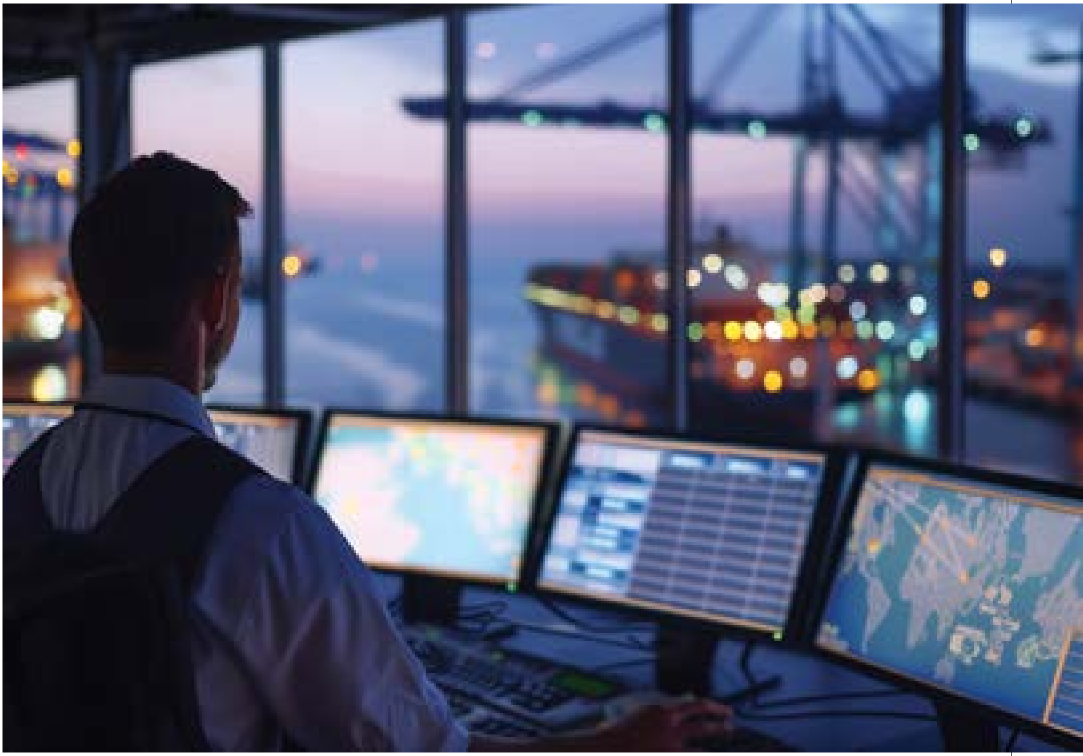
system reduces noise, clarifies details, and increases brightness while preserving the integrity of the footage. It does not imagine what is missing, it reveals what is already hidden beneath the noise of low light or sensor limitations.

This distinction is especially important when video footage might serve as forensic evidence. Enhancing visibility without altering content ensures that the output remains a truthful representation of the recorded scene, a key requirement for investigative and evidentiary use.

WHY AI EXCELS IN LOW-LIGHT IMAGING

Traditional image signal processors (ISPs) struggle to fully separate noise from signal, and amplifying the remaining signal also amplifies noise, degrading visual image quality. CNN-based systems, however, suppress noise so effectively that higher gain can be applied without sacrificing clarity. The





result is video that is not only sharper and clearer, but also significantly brighter, recovering usable details even in near-total darkness where human vision fails.

Unlike fixed-algorithm ISP pipelines, CNN-based methods are trained on diverse, low-light data with complex noise patterns and light distributions. Learning is supervised and uses noisy videos together with their clean counterparts so that the system can learn how to separate meaningful content from a poor quality video stream. This adaptive intelligence allows for more effective enhancement across challenging scenarios while preserving fidelity to the original scene.

In an era of deepfakes and synthetic imagery, it is crucial to distinguish

> IN AN ERA OF DEEPFAKES AND SYNTHETIC IMAGERY, IT IS CRUCIAL TO DISTINGUISH TECHNOLOGIES THAT MERELY ENHANCE VISIBILITY FROM THOSE THAT GENERATE NEW DATA.

technologies that actually enhance visibility from those that generate new data. CNN-based low-light enhancement offers a powerful, trustworthy solution, improving the clarity, brightness and usability of surveillance video while maintaining its evidentiary integrity.

REAL-WORLD USE CASES

CNN-based low-light enhancement plays a vital role across multiple real-world applications where operational accuracy is critical but visibility is limited.

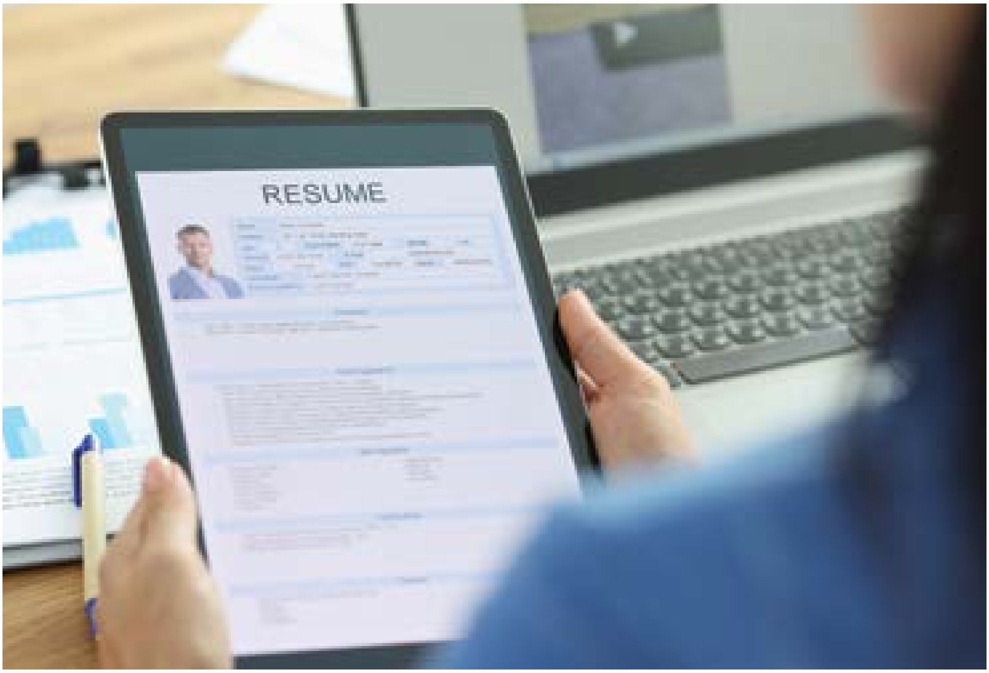
- In public safety and law enforcement, it enables surveillance in poorly lit areas, improving facial recognition, object identification, and video admissibility.
- Transportation systems benefit from enhanced camera feeds for night-time incident detection and safety in autonomous driving.
- Critical infrastructure sites, such as power plants and ports, require 24/7 monitoring, often in low-light conditions to reduce energy use and light pollution. CNN-enhanced footage ensures better detection of threats or anomalies without relying on thermal imaging.
- Border surveillance and military operations use real-time, low-light video to distinguish movements in remote or tactical environments where

artificial lighting could compromise security.

- In the retail and commercial sector, CNN-based enhancement improves security in dimly lit areas like warehouses and alleys, supporting both crime prevention and investigation.

In critical environments where security, accountability and clarity are non-negotiable, *how* video is enhanced is just as important as the outcome. CNN-based low-light enhancement offers a real-time approach that emphasizes signal fidelity rather than synthetic reconstruction. Unlike generative AI, which can introduce artificial elements, CNN methods are able to uncover what is actually present in the footage, strengthening operational decisions. As imaging technologies advance, this focus on preserving the authenticity of original footage ensures that improved visibility never compromises the truth. ◀

> IN CRITICAL ENVIRONMENTS WHERE SECURITY, ACCOUNTABILITY AND CLARITY ARE NON-NEGOTIABLE, *HOW* VIDEO IS ENHANCED IS JUST AS IMPORTANT AS THE OUTCOME.



A Digital Transformation in Talent

New technologies are changing the skillsets needed in the security industry

The world is undergoing a rapid digital transformation, and few sectors are feeling the shift more acutely than the security industry. A space that was once defined by physical presence and analog systems is now evolving into a high-tech ecosystem of sensors, AI, cloud-based platforms, and cybersecurity solutions. This shift is not just changing how the industry operates, it is redefining the kind of talent it needs.

The modern security landscape demands a new breed of professionals to tackle new areas of the sector, from smart surveillance to biometric authentication to threat detection powered by machine learning. Digital fluency is now just as critical as field experience. As the industry retools for a digital future, the competition to

Brett Ennals (be@centogroup.com) is the CEO of Cento (www.centogroup.com).

attract and retain top-tier, technologically proficient talent is intensifying.

Security has evolved from being manpower-heavy to tech-intensive, and organizations need to adapt to succeed.

THE DIGITAL SHIFT: MORE THAN CAMERAS AND ALARMS

For decades, the security sector was largely focused on physical protection – guards, patrols, locks and keys. Fire alarm engineers, CCTV installers, and access control specialists kept buildings and people safe by physically wiring systems, programming control panels, and conducting on-site inspections. But with the rise of connected devices, cloud infrastructure, and AI-driven analytics, today's security solutions are far more complex.

This transformation means that traditional skillsets alone no longer suffice. Security firms are now seeking engineers with technical knowledge, systems integrators with

> “DIGITAL FLUENCY IS NOW JUST AS CRITICAL AS FIELD EXPERIENCE.

technology expertise, and cybersecurity specialists – talent profiles traditionally more common in tech firms than in the security industry. The toolkit of a modern fire or security professional is no longer just physical, it is digital, too.

> THE EXPANDING DIGITAL LANDSCAPE IS PUTTING PRESSURE ON SECURITY COMPANIES TO RETHINK HOW THEY SOURCE, TRAIN AND RETAIN EMPLOYEES.

TALENT IN TRANSITION: A NEW INDUSTRY PLAYBOOK

The expanding digital landscape is putting pressure on security companies to rethink how they source, train and retain employees. The new workforce must be agile, tech-savvy and capable of adapting to rapidly evolving technologies.

The key, in-demand roles include:

- *Internet of Things (IoT) and systems engineers:* Security systems

are increasingly interconnected. Engineers who understand IoT architecture, cloud integration, and system interoperability are now fundamental to success.

- *AI & data specialists:* With data powering smart surveillance and behavior analysis, those who can build, train and maintain AI models are badly needed.
- *Specialists with technical expertise:* Professionals with technical knowledge are becoming essential to businesses. Those with a deeper understanding of security systems are standing out in the market.
- *Designers and digital product managers:* Security solutions are no longer solely hardware-based. Creating user-friendly interfaces for apps, dashboards and remote monitoring tools is becoming a core competency.
- *Executives and directors:* Individuals

THE INDUSTRY NEEDS PROFESSIONALS WHO UNDERSTAND BOTH THE PHYSICAL WORLD OF CABLING, CONTROL PANELS AND COMPLIANCE, AS WELL AS THE DIGITAL WORLD OF AI, DATA AND CLOUD.

who can lead digital adoption, oversee system transformation, and shape strategy around connected technologies and service-based business models are more valuable than ever today.

A GROWING TALENT GAP

One of the biggest challenges facing the security sector is the digital talent gap.

Many highly-skilled individuals entered the industry in an analog age and are now having to upskill quickly. At the same time, younger, tech-savvy talent often looks to more “glamorous” industries like fintech, gaming or consumer electronics, overlooking security as a career path altogether.

This creates a bottleneck, particularly in mid-level roles. The industry needs professionals who understand both the physical world of cabling, control panels and compliance, as well as the digital world of AI, data and cloud. These professionals are rare, and competition for them is intense.

ATTRACTING THE NEXT GENERATION

To compete for digital talent, the security

industry must rebrand itself – not just as a protector of people and property, but as a technology-driven, mission-critical field with global relevance.

Some key strategies for this include:

- *Modernize employer branding:* Emphasize innovation, impact and purpose. Young digital professionals are drawn to roles that make a difference, and security offers a clear value proposition in that regard.
- *Invest in upskilling and internal mobility:* Partner with tech education platforms, launch in-house academies, and create hybrid career pathways from traditional security to tech-centric roles to help bridge the skills gap internally.
- *Collaborate with universities and tech bootcamps:* Create tailored internships, capstone projects, or research partnerships to help funnel tech talent into the security pipeline early.
- *Flexible and remote work opportunities:*

> “
> THE LINE BETWEEN DIGITAL AND PHYSICAL THREATS IS BLURRING. … THE PROFESSIONALS EQUIPPED TO MANAGE THIS NEW THREAT LANDSCAPE MUST BE EQUALLY HYBRID IN THEIR CAPABILITIES.

In an increasingly remote-friendly job market, tech professionals expect flexibility. Security firms need to adapt their work structures and technology stacks to appeal to this expectation.

- *Showcase career growth and innovation:* Too often, security roles are viewed as static. Highlight opportunities for career progression, innovation labs, and cross-functional collaboration to help change that narrative. Let young talent see the industry as a place where they can grow, lead and innovate.

THE ROAD AHEAD

As digitalization accelerates, the security industry stands at a crossroads. Those who invest in digital transformation – not just through tools, but also through people – will lead the charge in creating safer, smarter environments for businesses and residents alike.

The line between digital and physical threats is blurring. A cyberattack can compromise a building's access control just as easily as a stolen badge can. The professionals equipped to manage this new threat landscape must be equally hybrid in their capabilities.

The winners in this next wave will not just be the firms with the best tech. It will be the ones who build teams that understand both the digital and human elements of security. It is a hybrid war, and it demands hybrid talent.

To stay competitive, the industry must broaden its definition of talent, rethink its hiring narratives, and embrace a digital-first mindset. Because in the security industry of tomorrow, guarding the front gate means guarding the firewall, too. ◀

Minimizing Disruption, Maximizing Learning

How advanced security solutions empower schools to focus on their core mission

Kristen Plitt (kplitt@idisamericas.com) is the Vice President of Marketing & Sales Development at IDIS Americas (https://idisamericas.com).

In today's educational landscape, the safety of students, staff and faculty is key. But this should never come at the cost of disrupting the true purpose of schools: learning.

K-12 establishments are adopting innovative security solutions that work seamlessly behind the scenes, ensuring that educational environments remain focused on providing a safe space for students to learn and grow. By integrating advanced technologies, schools can minimize disruptions while enhancing safety, allowing educators and students to stay focused on their academic goals.

THE SHIFT TOWARD INTEGRATED SECURITY

Traditional school security methods often focused on visible, intrusive measures that could

> BY INTEGRATING ADVANCED TECHNOLOGIES, SCHOOLS CAN MINIMIZE DISRUPTIONS WHILE ENHANCING SAFETY, ALLOWING EDUCATORS AND STUDENTS TO STAY FOCUSED ON THEIR ACADEMIC GOALS.

inadvertently disrupt the learning environment. However, advances in security technology prioritize unobtrusiveness. These solutions integrate seamlessly into the daily life and routine of schools, supporting safety without interrupting the natural flow of learning.

Modern video surveillance systems, for instance, offer high-definition footage and AI-driven analytics to identify potential security threats without requiring constant human oversight. These systems operate quietly in the background, providing real-time alerts to staff without interrupting classrooms or school activities. They ensure that safety is constantly maintained so that teachers can focus on teaching and students can focus on learning.

TECHNOLOGY NOW ALLOWS SCHOOLS TO CREATE AUTOMATED RESPONSE PLANS FOR EMERGENCIES LIKE LOCKDOWNS AND EVACUATIONS THAT CAN BE TRIGGERED INSTANTLY WHEN NEEDED.

SUPPORTING FOCUS WITH ACCESS CONTROL

Access control systems play a critical role in maintaining a secure, focused environment. Rather than relying on manual checks or disruptive measures, today's systems can automatically verify identity and grant access to authorized individuals. This means that students and staff can move freely throughout the campus without unnecessary barriers, while the system ensures that only authorized individuals can access restricted areas.

By integrating access control with video surveillance, schools can ensure that security is largely unseen. The seamless nature of these systems minimizes disruption while protecting

the integrity of the learning environment.

TECHNOLOGY-DRIVEN EMERGENCY RESPONSE

While prevention is essential, so is readiness for incidents. Emergency response systems are most effective when they work quietly and efficiently, especially during critical moments. Technology now allows schools to create automated response plans for emergencies like lockdowns and evacuations that can be triggered instantly when needed.

These systems are designed to be swift and discreet, ensuring that the learning experience is not interrupted unless and until it is necessary. They provide real-time communication, giving educators and administrators the tools

> “
>
> DATA FROM VIDEO SURVEILLANCE, ACCESS CONTROL SYSTEMS, AND EVEN EMERGENCY RESPONSE DRILLS CAN PROVIDE INSIGHTS THAT ENABLE SCHOOLS TO IDENTIFY AREAS OF IMPROVEMENT.

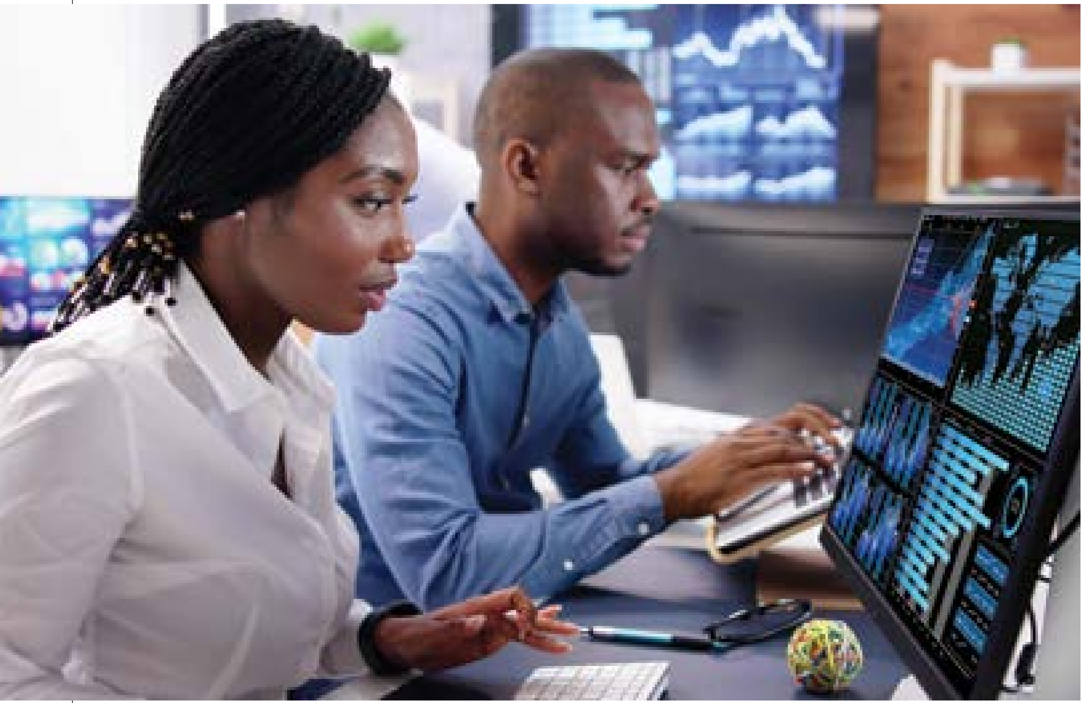
BUDGET CONSTRAINTS, PRIVACY CONCERNS, AND THE COMPLEXITY OF INTEGRATING NEW TECHNOLOGIES WITH EXISTING INFRASTRUCTURE ARE ALL VALID CONCERNS. HOWEVER … THESE CHALLENGES CAN BE OVERCOME.

they need to protect students while keeping them focused on their education.

ENHANCING LEARNING WITH DATA

Another advantage of modern security technologies is the ability to collect valuable data that can help schools refine their practices without affecting the learning environment. Data from video surveillance, access control systems, and even emergency response drills can provide insights that enable schools to identify areas of improvement without overhauling the entire system.

This information empowers school administrators to make informed decisions that enhance safety protocols while ensuring that the student experience remains uninterrupted. With real-time reporting



and predictive analytics, schools can stay ahead of potential threats while keeping the focus on fostering a thriving educational environment.

OVERCOMING CHALLENGES WHILE PRESERVING FOCUS

While technology offers significant benefits, it is important to address the challenges associated with integrating advanced systems into school environments. Budget constraints, privacy concerns, and the complexity of integrating new technologies with existing infrastructure are all valid concerns. However, when security solutions are implemented thoughtfully, these challenges can be overcome.

The key lies in ensuring that security measures are designed to be non-intrusive and compatible with the day-to-day flow of educational activities. School security should never be a distraction; instead, it should be a silent partner that helps ensure that safety and education go hand in hand.

The goal of any school security system is to create a safe environment where learning can be fun, and children can grow. By integrating advanced technologies that focus on efficiency, non-intrusiveness, and seamless operation, K-12 schools can prioritize education while ensuring safety. With the right security solutions in place, schools can protect students and staff without disrupting the educational experience. ◀

The Convergence of Vision, Intelligence and Agency

AI is reshaping physical security and humans' role in it

James Connor (james@ambient.ai) is the Head of Corporate Engagements at Ambient.ai (www.ambient.ai).

For years, the promise of AI has been quietly reshaping the digital world. Now, that influence is moving beyond the screen and into the physical spaces where we work, shop and live. This shift from bits to atoms is nowhere more apparent than in physical security, an industry on the cusp of its most significant transformation in a generation.

The days of reactive, forensic security are numbered. Today, AI is enabling a proactive, predictive posture that reshapes how organizations protect their people, property and infrastructure. At the heart of this evolution is computer vision, AI's ability to interpret and act on visual data in real time. This is not just about better automation; it is a fundamental convergence of physical security, cybersecurity and business intelligence. We are moving toward fully integrated threat detection and response ecosystems, and the implications for technology and talent are immense.

THREE FORCES DRIVING THE SHIFT

The move from AI experimentation to enterprise-scale deployment is not happening in a vacuum. It is the result of three powerful, converging trends.

> THIS SHIFT FROM BITS TO ATOMS IS NOWHERE MORE APPARENT THAN IN PHYSICAL SECURITY, AN INDUSTRY ON THE CUSP OF ITS MOST SIGNIFICANT TRANSFORMATION IN A GENERATION.

1. The rise of multimodal AI

The most advanced AI systems no longer operate on a single data stream. Multimodal AI fuses visual data from cameras with audio, text access control logs, and network data. This creates a rich, contextual understanding of the environment, allowing the system to make dynamic, real-time

FOR ENTERPRISE SECURITY LEADERS, A STRONG GOVERNANCE FRAMEWORK IS ESSENTIAL FOR ADOPTING AI RESPONSIBLY AND ENSURING THAT ITS OUTPUTS ARE FAIR, RELIABLE AND AUDITABLE.

decisions. Think of it as moving from a single-sense understanding of a situation to a full-sensory one, dramatically reducing false positives and identifying complex threats that would otherwise go unnoticed.

2. The mandate for AI governance

As AI becomes more powerful, the need for guardrails grows. Regulatory frameworks like the European Union's AI Act and recent presidential executive orders in the United States are pushing organizations toward transparency, ethical deployment, and risk mitigation. This is not a barrier to innovation; it is a catalyst for trust. For enterprise security leaders, a strong governance framework is essential for adopting AI responsibly and ensuring that its outputs are fair, reliable and auditable.

3. The autonomy of edge AI

Not all decisions need to travel to the cloud and

back. The proliferation of powerful processors allows for edge AI, where smart sensors, drones and robotic patrol units can make localized decisions instantly. This reduces latency, improves resilience (especially in low-connectivity areas), and ensures that critical alerts are processed on-site, enabling a faster, more effective response without cloud dependency.

AI-ENABLED CAPABILITIES

This convergence of technological forces is creating a new suite of tools that are redefining the capabilities of modern security programs.

- *Proactive surveillance through vision AI:* This is the foundational layer. Computer vision transforms surveillance cameras from passive recording devices into active, always-on sentinels. Instead of a human operator trying to monitor dozens of screens, the AI platform intelligently detects potential threats, such as unauthorized access, suspicious loitering, tampering, or brandishing of

> NEXT-GENERATION GSOCs ARE POWERED BY AI PLATFORMS THAT INTEGRATE VISION, ACCESS CONTROL, COMMUNICATIONS AND EVEN CYBER THREAT DATA INTO A SINGLE PANE OF GLASS.

weapons, and triggers immediate, targeted alerts. This allows security teams to focus on the signal, not the noise, and to intervene *before* an incident escalates.

- *Autonomous aerial and ground units:* AI-powered drones and robotic patrol pods are becoming powerful force multipliers. Equipped with thermal and advanced vision analytics, these units can conduct automated patrols of large perimeters, track threats in real time, and inspect hazardous environments, all while reducing the risk to human personnel. Integrated with a central AI platform, they provide an on-demand "eye in the sky" or a persistent ground presence that extends the reach of the security team.
- *Unified decision intelligence of the*

GSOC: The global security operations center (GSOC) is evolving from a monitoring hub into an intelligence nerve center. Next-generation GSOCs are powered by AI platforms that integrate vision, access control, communications and even cyber threat data into a single pane of glass. This provides operators with predictive situational awareness, allowing them to take action on a suspicious physical event and a potential digital attack vector, enabling a truly unified response.

CYBER-PHYSICAL CONVERGENCE: FROM SECURITY TO INTELLIGENCE OPERATIONS

The most damaging and costly breaches often start with a simple physical lapse: a tailgater slipping through a door, a sensitive document left on a printer, an unauthorized device connected to a port. For too long, physical security and cybersecurity have operated in silos. This is no longer a viable strategy.

These events are not isolated risks; they are

AI – COMPUTER VISION, IN PARTICULAR – IS THE BRIDGE THAT FINALLY CONNECTS THE TWO DOMAINS. IT ALLOWS ORGANIZATIONS TO ACHIEVE TRUE CYBER-PHYSICAL THREAT CORRELATION.

entry points to systemic compromise.

AI – computer vision, in particular – is the bridge that finally connects the two domains. It allows organizations to achieve true cyber-physical threat correlation. For example, an AI platform can:

- Flag an access control event where one person's badge is used, but the camera feed shows a different person (or multiple people) entering
- Detect an individual accessing a server room after hours and correlate it with anomalous network activity originating from that same location
- Identify reconnaissance behavior, such as someone taking photos of secure areas or attempting to access restricted zones repeatedly

HUMAN AGENCY SCALE (HAS) FRAMEWORK

HAS Level	Meaning	Security Application Example
H1	Full AI Autonomy	AI automatically locks down a perimeter upon detecting a weapon
H2	Minimal Human Input	AI detects a vehicle in a no-park zone and dispatches a patrol after a timer expires
H3	Equal Partnership	AI flags an after-hours access event; a human operator correlates it with a work order
H4	Human-Led Task	An operator uses AI to quickly search for a person of interest across all cameras
H5	Essential Human Involvement	A human guard uses their intuition to de-escalate a tense situation, with AI providing background data

This marks a profound shift in thinking, from running separate security operations to managing a unified intelligence operation, where all data converges to create a complete picture of the threat landscape.

THE HUMAN FACTOR: AUGMENTING TALENT, NOT REPLACING IT

Perhaps the most critical aspect of this transformation is its impact on people. The narrative of AI replacing jobs is outdated and incomplete. In physical security, AI is augmenting human talent, offloading repetitive, low-value tasks and elevating human operators into more strategic roles.

Frontline staff can now shift from being passive monitors to becoming vision system operators, cyber-physical threat analysts, and human-robot interaction specialists. This evolution requires a new focus on reskilling and a framework for managing the partnership between people and machines.

To guide this transition, leading organizations are adopting the Human Agency Scale (HAS), a framework for determining the appropriate level of human involvement for any given AI-enabled task.

The HAS framework shifts the question from “Can we automate this?”

> ORGANIZATIONS THAT EMBRACE THIS NEW PARADIGM, TREATING AI NOT AS A REPLACEMENT FOR PEOPLE, BUT AS A TOOL TO ELEVATE HUMAN JUDGMENT, WILL LEAD THE WAY.

to “Should we automate this, and to what degree?” It ensures that human judgment, intuition and context awareness remain central to the security mission, fostering trust and preventing the blind spots that can arise from over-automation.

FUNDING INTELLIGENCE THROUGH RISK AVOIDANCE

Ultimately, the adoption of a vision-driven security strategy is a business decision. With the average cost of a cyber breach now at $4.8 million, a proactive investment in an AI-powered physical security platform, which can prevent the incidents that lead to such breaches, offers an undeniable return on investment.

Security is no longer a cost center; it is a business

intelligence function that avoids catastrophic losses, protects brand reputation, and optimizes operational uptime. By building a strategic roadmap that invests in human-AI collaboration, establishes strong AI governance, and engineers safe human-robot workspaces, organizations can unlock immense value.

VISION IS THE INTERFACE, HUMAN AGENCY IS THE COMPASS

The future of security is here, and it is powered by computer vision. But technology alone is not the answer. Vision AI is the catalyst that enables us to see more and react faster, but it is human agency that provides the guidance to implement it responsibly and effectively.

Organizations that embrace this new paradigm, treating AI not as a replacement for people, but as a tool to elevate human judgment, will lead the way. They will move beyond the old model of “react and record” to a future of “predict and prevent,” one powered by the unmatched combination of artificial intelligence and human wisdom. ◀

Selling Security to the C-Suite

Successful approaches demonstrate impact on operations and revenue

For too long, organizations viewed security as a cost center, which meant that the department was forced to take a backseat to those that made money.

But this is not the case anymore.

Security leaders are no longer limited to leading security efforts. More than ever, these individuals are business leaders who wear a security hat. This means that their job is to create value for the business, contribute to the bottom line, and speak the C-suite language when it comes to investing in technology that addresses business risk.

Their impact is vast, and it means security does not slink into the background of the organization anymore. It is a highly visible endeavor to lead these teams – and it takes someone who understands the business, its goals, and how to support them.

Ryan Schonfeld (info@hivewatch.com) is the Co-Founder & CEO of HiveWatch (www.hivewatch.com).

Security leaders need to take multiple factors into consideration when discussing technology investments with the C-suite.

THE CLOSER YOU CAN TIE SECURITY TO REVENUE GENERATION, THE MORE SUCCESSFUL YOU ARE GOING TO BE.

QUANTIFY IMPACT ON OTHER BUSINESS FUNCTIONS

Demonstrating that a robust business impact analysis has been done to quantify the impacts of security – including on other business functions – can be compelling.

One example of this might be using security data to better manage the facility. Understanding how many people are utilizing a space can help businesses decide whether it is prudent to have a physical presence or can alert facility managers to underutilized areas, which could ultimately lead to cost savings on rent or lease of the space. It can also have a significant impact on energy efficiency, which can affect a business's bottom line.

WITHOUT THE FORETHOUGHT TO CREATE A FOUNDATION FOR SCALABLE SECURITY, ORGANIZATIONS MAY PAY A LOT MORE FOR THE SAME LEVEL OF PROTECTION.

CONNECT SECURITY TO BUSINESS CONTINUITY

It is an easy sell if security technology investments are being driven by a regulatory requirement and there are consequences for not complying. Also, if a business is experiencing significant monetary losses because of an unaddressed physical security problem, that is something security leaders would definitely have to mitigate. This kind of loss can be presented in dollar terms.

On top of that, there are business continuity issues to consider. For example, online and physical data must be kept secure. If somebody breaks into a data center, security will help to protect the information and keep the business operating. Scenarios like this make security technology easier to sell.

Security also has a clear role in meeting the increasing need for

executive protection, a risk that can be very personal for decision-makers.

RECRUIT CHAMPIONS IN OTHER DEPARTMENTS

Security leaders should ask several questions of people internally, including:

- What am I solving for?
- What risk?
  What issue?
  What regulatory requirement?
- Am I replacing something?
- Do we already have a solution that is just not working?
- Is there going to be overlap and spend while bringing on a new solution?
- What are the benefits of that?

Once these questions are answered, then the organization is really able to drive people to make sure they have done their homework – and leadership is better able to hold people accountable to the results of that.

It is very important to make sure that security leadership has a package in place and a plan for achieving buy-in from other internal influencers. Without that buy-in across the organization, the adoption of technology will be lacking, and implementing additional steps will be harder. While the executive team holds a lot of power and influence, they also typically rely on a feedback loop for things happening within the organization. And sometimes those right-hand people are more dialed into conversations about what has been occurring.

CONNECT SECURITY TO REVENUE GENERATION

The closer you can tie security to revenue generation, the more successful you are going to be. Security leaders need to understand the business and think like both stakeholders and customers.

Consider what is creating profit for the business. Ask:

- What is it that we need?
- Do we need more customers?
- Do we need to reduce costs?

- How can a security solution fit into that?

When thinking about it from the customer's perspective, trust is everything. In the financial services space, for example, security can be closely related to revenue generation since having better security is a key selling point to customers. A security solution that increases efficiency, meanwhile, can reduce overall costs and improve profits.

These are the kinds of things that get a security solution approved.

COMMUNICATE SCALABILITY AND CONSIDER REPUTATIONAL RISK

Another way to speak the C-suite language is by focusing on building blocks and prioritizing investments that allow for scalability. When building security programs, if leaders do not get the basics right, it can often cost the organization a significant amount of money to start over with that function, whether it be travel security, workplace safety, prevention, event security, THE TCO REVEALS WHETHER A SECURITY INVESTMENT IS A STRATEGIC ASSET OR A MONEY PIT.

or another area. Security touches every facet of the organization and without the forethought to create a foundation for scalable security, organizations may pay a lot more for the same level of protection.

In many cases, it is important to communicate to the executive team, "Let's do things right at the onset to save ourselves a lot of heartache in a couple of years." Any security leader can tell you about the high cost of investing in a cheap solution.

The last piece, which often gets overlooked, is consideration of reputational risk.

Using benchmarking to communicate the value of an investment works well and resonates with leaders. Answer questions such as:

- What is the impact, reputationally, if we do not effectively invest in security?
- How can we benefit if we effectively invest in tools that make doing business easier?

DETERMINE TOTAL COST OF OWNERSHIP

Security can be high stakes, but as we see budgets shrink and finance departments push back on new investments, it is time to consider the total cost of ownership (TCO) of projects. The TCO reveals whether a security investment is a strategic asset or a money pit. The analysis cuts through the noise to show why technology – such as platforms to manage incident management and response – are fundamentally changing the economics of protection in ways that traditional approaches simply cannot.

Organizations seeking to optimize security technology TCO should consider these strategic approaches:

- *A platform-first strategy:* Rather than purchasing point solutions and then struggling with integration, start with a robust security operations management platform that provides the foundation for the security ecosystem. This ensures that new technologies can be seamlessly incorporated as needed.
- *Engage in return on investment (ROI)-based evaluation:* Assess security technology based on comprehensive ROI calculations that include all TCO factors, not just purchase price. The lowest initial cost rarely delivers the best long-term value.
- *Create ongoing operational impact analyses:* Evaluate how security technology choices will affect daily operations, including staffing requirements, training needs, and response capabilities. Operational efficiency is often the largest component of long-term TCO.
- *Allow for scalability planning:* Select security technology with future growth

> THE TRANSFORMATION OF SECURITY FROM A COST CENTER TO A STRATEGIC BUSINESS DRIVER REPRESENTS ONE OF THE MOST SIGNIFICANT SHIFTS IN MODERN ORGANIZATIONAL THINKING.

in mind. Solutions that require complete replacement rather than expansion as the organization expands create substantial unnecessary costs.

INVEST STRATEGICALLY, NOT REACTIVELY

The transformation of security from a cost center to a strategic business driver represents one of the most significant shifts in modern organizational thinking. Security leaders who successfully engage C-suite executives understand that their role extends far beyond traditional protection. They must demonstrate quantifiable business impact, connect security initiatives to revenue generation, and build cross-departmental champions who recognize security's value in supporting core business functions.

By framing security investments through the lens of business continuity, regulatory compliance, loss prevention, and competitive advantage, these leaders position security as an essential component of sustainable growth rather than a necessary expense.

C-suite executives must recognize that security is not just about preventing losses but about enabling business growth, maintaining customer trust, and building operational resilience in an increasingly complex threat landscape. Organizations that view security through a strategic lens, investing in scalable platforms and comprehensive solutions rather than piecemeal fixes, position themselves for long-term success, while those that treat security as an afterthought face mounting risks that threaten their very survival. The question is no longer whether to invest in security, but how quickly leaders can align their security strategy with their business strategy to unlock the full potential of both. ◀