

AI Hype vs. Reality in Retail Security

What actually works today,
and how can it benefit your stores?

PRODUCED BY



SIA

RETAIL SECURITY
ADVISORY BOARD

SIA's Retail Security Advisory Board brings together retailers and security solutions providers to foster collaboration, develop best practices and address key challenges such as organized retail crime.



Contents

Introduction	2
Terminology Distinctions	3
Moving from Understanding to Implementation	4
Implementation: What Technology is Being Used?	4
AI-Powered Exception-Based Reporting	4
Alarm Monitoring and Automated Deterrence	5
Automated Store Audits and Shelf Compliance	5
Customer Experience and Store Performance Analytics	6
Facial Recognition Technology (FRT)	6
License Plate Recognition (LPR/ALPR) and Vehicle Detection	7
Natural Language Video Search	7
Self-Checkout Monitoring	8
How Does This Help Retailers Today?	9
Greater Output With Fewer Resources	9
Reduced Dependence on Physical Guarding	9
Real-Time Store Optimization	9
Adding Context to Shrink Metrics	10
Security as a Revenue Contributor	10
Limitations	11
AI Accuracy	11
Operational Gaps	11
Not All AI Is Equal	11
Expectations	12
Data Privacy	12
Policy and Governance	13
Final Thoughts & Key Takeaways	14
Key Takeaways for Retail Leadership	14
Key Takeaways for Integrators	15
Key Takeaways for Suppliers	15
Key Takeaways for Corporate Stakeholders	15

Introduction

Artificial intelligence (AI) is one of the most talked-about technologies in retail operations and security today and one of the most misunderstood. Headlines promise transformation, technology and solution suppliers promise precision, and internal stakeholders are asking a simple question: What actually works, and how does it impact our stores today?

This paper was developed by the Security Industry Association (SIA) Retail Security Advisory Board to cut through the noise. The purpose is to provide asset protection, store operations and technology leaders with a clear, practical understanding of basic AI terms and highlight how AI is being used in retail environments today, where it delivers real value, where it falls short and how to evaluate it responsibly.

The goal of this paper is not to promote the hype or position AI as a replacement for retail teams. AI is not a future-state concept—it is already embedded in many retail environments today. Instead, this resource is designed to provide a grounded, real-world perspective on how AI can serve as a practical tool when paired with clear business objectives, strong workflows and realistic expectations.



Terminology Distinctions

In the context of modern retail security, the distinction between analytics, machine learning models, AI, generative AI and agentic AI is defined by a progression from simple detection to complex synthesis. Understanding these differences is important, not only for evaluating technology and solution suppliers and providers, but also for setting realistic operational and loss prevention expectations that can genuinely improve safety, reduce shrink, enhance operational visibility and support better decision making. While there are many acceptable and various definitions of the terms below, this paper uses language and context from the SIA AI Advisory Board to follow industry standards.

- **Analytics** involves the automated processing of data to identify specific temporal or spatial events. In a retail environment, this typically manifests as rule-based “tripwires” or sensors—systems that can count foot traffic or alert staff when a restricted door is opened but lack the nuance to interpret the intent behind or broader context around the movement.
- **Machine learning (ML)** models represent the next step, acting as the essential engine that allows systems to distinguish specific patterns and visual elements within a given data source. In video surveillance, machine learning moves past simple motion detection to identify specific physical attributes. For example, ML helps a system isolate a person wearing a hat, sunglasses, blue shoes or a short-sleeve shirt or identify objects such as a green motorcycle or a briefcase. This level of learning is foundational for training systems to recognize characteristics from prior incidents and to generate alarms in real time should a specific set of visual conditions be observed.
- **Artificial intelligence** serves as a broader technological umbrella, encompassing systems capable of performing tasks that traditionally require human intelligence, such as visual perception and decision making. Unlike basic analytics, AI uses machine learning and computer vision to recognize complex patterns. In practice, this allows a retail security system to go beyond mere motion detection to identify specific behaviors, such as “sweethearting” at the point of sale or recognizing the faces of known organized retail crime (ORC) offenders. While analytics identifies that an event occurred, AI understands what is occurring and identifies the subjects involved.
- **Generative AI** shifts the focus from static recognition to creative synthesis and proactive problem solving. Where traditional AI classifies existing data, generative AI translates vast pools of raw security metadata into strategic intelligence. In an ideal retail environment, generative AI bridges the gap between raw footage and actionable loss prevention. For example, a surveillance system’s metadata (e.g., logs of events, times, recognized objects and behaviors) can be automatically translated into human-readable text. Generative AI then interprets this narrative leveraging its extensive training data, past incident history and situational information to deduce the possible outcome of an unfolding situation on CCTV.
- **Agentic AI** moves from systems that just give advice to systems that can take action completely on their own. While generative AI explains data and suggests solutions, agentic AI acts on those insights independently by connecting directly to your store’s security infrastructure including cameras, electronic locks and communication networks. For retail security leaders, this technology transforms traditional workflows from human-dependent monitoring into real-time, automated incident response. For example, during a late-night break-in at a closed storefront, an agentic AI system does not just alert a manager—it instantly executes a set of procedures such as broadcasting a targeted voice warning over the store speakers, locking electronic gates to contain the suspect and notifying law enforcement with a text-summarized feed of the incident.

Moving From Understanding to Implementation

It is a misconception that AI can fully replace human decision making. While AI can improve visibility, automate repetitive tasks and help prioritize events, human oversight remains essential in most retail environments today. Establishing clear policies and procedures for interpreting and acting on AI-generated insights is therefore critical. Before implementing any AI solution, organizations should consider:

- What data is being collected and analyzed? Who has access to that data?
- What regulatory or compliance requirements apply?
- Will your corporation's AI policy be published internally and externally for clarity and transparency?
- Are existing policies sufficient to govern the use of the technology?
- How will decisions and outcomes be audited or reviewed?
- Who owns the technology, the outcomes and the ongoing governance of the solution?
- How are responsibilities and liabilities defined between the organization and the solution provider?
- Have you formed a working group with HR, operations and legal to discuss AI plans, protocols and procedures?

While these considerations are essential for responsible adoption, they should not overshadow the practical value AI can provide. Establishing the right foundation ensures AI is deployed where it can deliver measurable outcomes and meaningfully support security operations. With the right approach, AI can serve as a practical tool to enhance decision making, improve visibility and support retail teams.



Implementation: What Technology Is Being Used?

AI-Powered Exception-Based Reporting

- **DESCRIPTION:** AI platforms that analyze transaction data, video and behavioral patterns to identify and prioritize potential investigations for loss prevention teams.
- **HOW IT WORKS:** The system flags anomalies such as excessive voids, high-dollar refunds, transactions processed without a customer present or patterns that suggest "sweethearting" (collusion between staff and customers). AI ranks these exceptions by severity, dollar impact, or likelihood of repeat offending, presenting loss prevention teams with a prioritized case queue rather than a wall of raw data.
- **ADVANTAGES:** Compresses investigation resolution time from hours to minutes and allows loss prevention teams to handle higher caseloads without adding headcount. Pairs transaction data with video evidence, enabling investigators to see the "who, what and how" behind each flagged event.
- **GUIDANCE:** Cannot determine intent or distinguish between honest mistakes and deliberate theft. Effectiveness degrades significantly when underlying POS data is incomplete, inconsistent or poorly structured, or when video is not integrated.

Alarm Monitoring and Automated Deterrence

- **DESCRIPTION:** AI-powered perimeter and interior security systems that combine autonomous detection with trained human monitoring to verify threats and respond in real time.
- **HOW IT WORKS:** AI-enabled cameras distinguish genuine threats from environmental noise (e.g., a cat walking past the entrance, a flag waving in the wind or an oscillating fan will not trigger an alarm, but a person approaching with a weapon, repeatedly peering into windows or setting up an encampment in an entryway will). When a legitimate threat is identified, the system can automatically deploy a staged response: activating strobe lights, issuing a customized audio warning over a speaker (e.g., addressing a specific individual by their clothing) and escalating to a live intervention specialist who can coordinate with law enforcement if the activity persists.
- **ADVANTAGES:** Resolves the vast majority of perimeter security events without requiring police dispatch and dramatically reduces false alarm costs and response burdens. This also extends coverage to after-hours periods when staffing is limited or absent and provides consistent, 24/7 protection across multiple locations. Lastly, it provides a cheaper alternative to hiring third-party guards.
- **GUIDANCE:** Cannot physically intervene or prevent a threat actor from entering or acting once on premises. Response effectiveness is dependent on the quality and placement of existing camera and speaker infrastructure as well as security operations center staffing and procedures.



Automated Store Audits and Shelf Compliance

- **DESCRIPTION:** AI-powered image recognition that automates shelf audits by analyzing photos to verify planogram compliance (map of how products are to be placed on store shelves), detect out-of-stock events, flag pricing errors and identify missing signage.
- **HOW IT WORKS:** Store associates or fixed cameras capture shelf images, and AI systems instantly compare them against expected layouts. Deviations are flagged in real time, and corrective tasks can be automatically assigned to the appropriate staff.
- **ADVANTAGES:** Reduces the time and labor cost of manual audits while improving accuracy and coverage. Retailers using automated shelf monitoring report significantly faster detection of out-of-stock conditions and real-time visibility into store conditions across all locations.
- **GUIDANCE:** Cannot reliably audit shelves with poor image quality, inconsistent lighting or cluttered facings. If packaging shape, size or color changes, this can disrupt the classification of multiple types as the same product. Does not understand why a deviation occurred, only that one exists. Cannot self-correct planogram data or inventory records. RFID might serve as a more robust and effective solution to out-of-stock issues.





Customer Experience and Store Performance Analytics

- **DESCRIPTION:** Analysis of video and sensor data to generate operational intelligence on customer behavior, staff performance and store conditions.
- **HOW IT WORKS:** Camera-based analytics generate data on heat mapping (where customers spend time), queue management (how long checkout lines are), customer traffic patterns (peak hours, conversion rates) and employee compliance (whether stores are being opened on time and cleaned according to schedule, or whether staff are greeting customers as required).
- **ADVANTAGES:** Reduces or eliminates the need for expensive and often inaccurate “mystery shopper” programs (where companies hire undercover evaluators to act as regular customers) by providing objective, continuous, and scalable measurement of in-store execution. Also removes reliance on manual checklists submitted by store associates, which are prone to self-reporting bias and inconsistent completion.
- **GUIDANCE:** Measures only physical behavior and presence, not customer sentiment or satisfaction. Conversion rate data reflects traffic patterns but cannot account for why a customer left without purchasing. Queue time measurement does not capture customer tolerance thresholds, which vary significantly by store format, demographic and shopping mission.

Facial Recognition Technology (FRT)

- **DESCRIPTION:** Software analyzes facial features to match individuals entering a store against a database of known offenders enrolled for probable cause, such as individuals involved in violent incidents or organized retail crime—which is used widely in loss prevention programs. Note that other common use cases include video system features allowing rapid sorting and matching of images within recorded video data to assist with incident investigations, as well as access control systems that include biometric matching for employee access to secured areas.
- **HOW IT WORKS:** High-resolution cameras at store entrances capture images of individuals and compare them against a retailer-curated watchlist. When a probable match is detected, trained staff receive an alert with prior incident context and response guidance for human review, decision making and response.
- **ADVANTAGES:** Enables timely alerts for the small percentage of repeat offenders responsible for a disproportionate share of retail loss and violence. By targeting only this high-impact group, FRT helps retailers prevent violence and theft, investigate losses and increase prosecutions and recoveries. Effective use with guardrails, will also allow retailers to reduce the costs associated with lower-level personnel tasked with manual camera review and floor walking.
- **GUIDANCE:** After a probable match is detected, human verification is a must before any actions are taken. Note that such commercial use of facial recognition technology is legal in all 50 U.S. states (though prohibited in just several local

jurisdictions), and practical in all states except Illinois due to constraints under its Biometric Information Privacy Act.

License Plate Recognition (LPR/ALPR) and Vehicle Detection

- **DESCRIPTION:** AI-powered analysis of vehicle license plates in parking lots and loading docks to identify vehicles associated with organized retail crime or other prior incidents.
- **HOW IT WORKS:** LPR cameras capture plate data and compare it against watchlists in real time and can also keep a record of plate reads for retroactive analysis during security investigations.
- **ADVANTAGES:** Extends the security perimeter beyond the four walls of the store. Provides early warning before a threat actor even enters the building, giving teams more time to prepare and respond. When an incident does occur, LPR data helps investigators quickly identify who was involved by tying vehicle information to the event, which strengthens case building and supports faster resolution with law enforcement.
- **GUIDANCE:** Cannot identify individuals—only vehicles. A plate match does not confirm who was driving or whether that person entered the store. Dirty or obstructed plates, glare, fog, rain, shadows and camera angles can all affect plate readability. Effectiveness for real time alerting is dependent on watchlist quality, which most retailers cannot maintain without active law enforcement partnership. Ensure LPR data is managed in compliance with applicable privacy requirements and retention policies. Coordinate with law enforcement on watchlist management and data-sharing protocols.



Natural Language Video Search

- **DESCRIPTION:** The application of generative AI and large language models (LLMs) to allow security personnel to search through vast archives of video footage using conversational, plain-English queries. Instead of manually scrubbing through hours of tape or setting complex filters, users can “ask” the surveillance system for specific insights.
- **HOW IT WORKS:** The system uses a “vision-language model” that bridges the gap between video pixels and human language. The AI continuously analyzes video streams, converting visual actions into searchable text metadata. When a user types a query, such as “Find a man in a red hoodie carrying an oversized duffle bag near the electronics aisle,” the generative AI understands the semantic meaning of the request and instantly retrieves the most relevant video clips from across the entire store network.
- **ADVANTAGES:** This technology drastically reduces mean time to investigate. In traditional systems, finding a specific event can take hours of manual labor; with generative AI search, it takes seconds.



Use of this technology empowers nontechnical staff (such as store managers or floor leads) to perform complex forensic audits without specialized training. Furthermore, it enables “cross-camera tracking,” allowing security teams to quickly reconstruct an individual’s entire path through a store by simply describing their appearance.

- **GUIDANCE:** The system may surface inaccurate data or footage in its present-day form. Performance degrades substantially with low-resolution, poorly angled or legacy camera infrastructure.

Self-Checkout Monitoring

- **DESCRIPTION:** Computer vision systems that monitor self-checkout lanes in real time, flagging non-scans, item switching and other forms of missed payment at the point of sale.
- **HOW IT WORKS:** Overhead cameras track items as they move from cart to scanner to bagging area. If an item bypasses the scanner or the wrong barcode is used, the system flags the transaction and sends a real-time alert to an associate’s handheld device. The associate can then approach the customer with a nonconfrontational “customer service” interaction rather than an accusatory stop. This preserves the customer experience while addressing the loss event in the moment.
- **ADVANTAGES:** Allows retailers to keep self-checkout lanes open and staffed at lower levels without absorbing the loss that traditionally comes with reduced oversight. Protects the convenience and speed that customers expect from self-checkout while closing the gap that makes these lanes a high-shrink area.
- **GUIDANCE:** High false positive rates remain a persistent challenge across technology and solution suppliers. Systems are reliant on very specific camera angles above the register. Having robust processes in place for human review and mitigation of any false alerts is critical. Non apparel retail may experience a higher rate of success than apparel retail. Weighted scales and security tag removal add additional complexities.

Please note, all organizations should implement principles such as accuracy and accountability in surveillance systems, regularly auditing for biases, errors, transparency, hallucinations, etc.; keeping a human in the loop; and training the system to reduce such risks.

How Does This Help Retailers Today?

AI adoption in retail is accelerating, and the impact is becoming measurable. According to the results of NVIDIA's 2026 State of AI in Retail and CPG survey, 89% of retail industry leaders said AI has helped increase revenue, and 95% said it has helped reduce annual costs. Among retail and consumer packaged goods companies specifically, 37% reported cost reductions greater than 10%. Here are several areas where retailers are seeing measurable impact:

Greater Output With Fewer Resources

Retail security and operations teams are being asked to cover more locations with flat or shrinking headcount. AI does not replace these teams, but it changes what they spend their time on. Instead of manually reviewing footage, writing reports from scratch or monitoring camera feeds in real time, practitioners can focus on higher-value work such as case building, law enforcement coordination and strategic planning.

Reduced Dependence on Physical Guarding

A single on-site security guard can represent a significant recurring monthly expense when factoring in wages, benefits, scheduling overhead, and turnover, while covering only one location, one shift and one vantage point. AI-powered remote monitoring extends that coverage across dozens or hundreds of locations simultaneously. The 2026 Interface Systems benchmark, based on 1.6 million events across 18,258 U.S. retail locations, found that AI-powered perimeter protection resolved 96.1% of threats automatically, and interactive remote video monitoring resolved 62.4% of high-priority events without police dispatch.

Real-Time Store Optimization

Retailers have historically relied on lagging indicators such as monthly sales reports, quarterly mystery shopper scores, annual shrink data and associate-submitted checklists to understand what is happening inside their stores. AI replaces that feedback loop with continuous, real-time data on queue lengths, customer wait times, traffic flow and task completion. The data gives store operations, visual merchants, marketing and field leaders the ability to make adjustments in hours instead of quarters. In just one example, Winters Market, a small independent grocer in Northern California, went from losing \$40,000 a year with no visibility into what was happening on the floor to receiving real-time alerts that enabled same-day intervention.

89%

of retail industry
leaders said AI has
helped increase
revenue

95%

of retail industry
leaders said
AI has helped
reduce costs

**The Appriss
Retail 2026
Total Retail Loss
Benchmark
Report found
that 73% of the
\$90 billion in U.S.
retail shrink was
preventable.**

Adding Context to Shrink Metrics

Traditional shrink measurement tells retailers what they lost but rarely explains why. AI changes this by correlating data across video, POS transactions, access logs, staffing levels and time of day to surface the root causes behind loss patterns. A spike in shrink at one location might trace back to a staffing gap during shift change, a blind spot created by a recent planogram reset or a self-checkout lane that consistently goes unmonitored during peak hours. The Appriss Retail 2026 Total Retail Loss Benchmark Report found that 73% of the \$90 billion in U.S. retail shrink was preventable, but preventing it requires understanding the specific operational conditions that allowed it to happen

Security as a Revenue Contributor

One of the most significant shifts AI enables is repositioning the security function from pure cost avoidance to measurable business contribution. The same systems that detect theft can also surface insights on customer traffic, product placement, staffing gaps and operational compliance. This provides security leaders with data they can bring to conversations with merchants, operations and executive leadership.



Limitations

AI Accuracy

AI accuracy is probably one of the most misunderstood topics in retail right now. Almost every platform in the market is being labeled as “AI-powered,” but very few conversations focus on the conditions required for those systems to perform effectively in real operational environments. The reality is simple: AI is only as good as the environment it operates in. Camera placement matters. Lighting matters. Store layout matters. Camera quality and scene activity matter. A controlled demo environment during a presentation may be completely different from a live retail floor during peak business hours.

One of the biggest misconceptions retailers have going into evaluations is expecting perfect accuracy from day one. That is not realistic. Most AI platforms require time to process data, learn environmental patterns and adapt to operational conditions. Even then, false positives and missed detections remain part of the reality across nearly every platform in the market today. Retailers should also be cautious about evaluating solutions based only on polished demonstrations. Many platforms perform extremely well in controlled environments, but operational performance at scale is what ultimately matters. A successful demo does not automatically translate into consistent results across hundreds or thousands of locations.

Operational Gaps

Another important consideration is that AI does not automatically fix operational gaps. Poor camera positioning, inconsistent coverage, obstructed views, low image quality and challenging lighting conditions create problems for both human operators and AI models alike. Integration also plays a significant role in long-term success. Many AI platforms depend heavily on existing infrastructure, including cameras, VMS platforms, network environments, reporting workflows and operational processes. Even strong AI solutions can struggle if the surrounding environment and supporting systems are not properly aligned.

Not All AI Is Equal

Retailers should also recognize that not every AI solution marketed as AI is truly leveraging advanced AI capabilities, as many platforms still rely heavily on rule-based analytics or predefined logic and require human oversight and analysis. The goal should not be perfection—it should be operational improvement. If a solution helps reduce investigative time, improve event visibility, prioritize incidents more quickly or eliminate repetitive manual review, that creates measurable value. But expecting AI to operate flawlessly in every environment will often lead to failed evaluations, unrealistic expectations and poor long-term adoption outcomes.



The strongest deployments typically happen when:

- Expectations are aligned early
- Success metrics are clearly defined
- Communication remains consistent
- Both sides understand operational realities
- Limitations are discussed honestly
- Timelines are realistic
- Ownership exists on both sides
- Legal and Privacy Considerations

Expectations

One of the biggest reasons AI initiatives can struggle in retail is not because the technology fails. It is because expectations between the retailer and the technology and solution suppliers were never aligned from the beginning. Both sides typically enter a pilot with very different assumptions: technology and solution suppliers are often focused on speed, deployment timelines, proving value quickly and moving projects toward expansion. Retailers, on the other hand, are balancing operational priorities, internal approvals, security reviews, budgeting, store impact and long-term scalability discussions at the same time. Neither side is necessarily wrong, but when expectations are not clearly communicated early, the relationship can become strained.

From the technology and solution suppliers side, there must be an understanding that retail environments are operationally complex. Decisions are rarely made by one person, and even successful pilots may still require multiple layers of internal review before expansion decisions are made. At the same time, retailers expect transparency from suppliers around limitations, implementation requirements, learning periods, integration needs and realistic outcomes. Overselling capabilities during the sales process often creates long-term trust issues that are difficult to recover from later.

Retailers also play a major role in the success or failure of AI pilots. Organizations should not expect platforms to operate perfectly with minimal involvement or unrealistic timelines. Successful evaluations require internal ownership, clear communication, operational feedback, measurable success criteria and a clearly defined business problem from the start. The organizations seeing the best long-term results are typically the ones treating the process as a collaborative partnership rather than a simple product evaluation.

As AI capabilities continue to advance, organizations must evaluate more than just functionality and performance. Privacy and compliance considerations, legal obligations and internal governance policies should be part of every AI evaluation process from the beginning.

Data Privacy

Many AI solutions rely on large volumes of data, including video, images, transaction information and behavioral patterns. Organizations should understand potential risks related to data privacy, employee monitoring, customer rights, record retention requirements and emerging AI regulations. It is also essential to understand what data is being collected, who has access to it, how it is stored and how long it is retained. As adoption accelerates, organizations may face increased scrutiny regarding how decisions are made, how data is used and whether appropriate oversight exists.

Privacy laws worldwide share common principles. They establish a foundation for the lawful, fair, and responsible processing of personal information, including its collection, use, security and retention.

1. **Fairness and Transparency:** Process lawfully, fairly and in a transparent manner.
2. **Minimization:** Collect only what is necessary for intended and disclosed purposes.
3. **Purpose Limitation:** Use only for the intended and disclosed purposes.
4. **Accuracy:** Keep accurate, complete and up to date.
5. **Retention:** Retain only as long as needed, then securely delete or anonymize.
6. **Security:** Protect with safeguards against unauthorized access, loss or misuse.
7. **Accountability:** Demonstrate compliance through governance, risk assessments and policy enforcement with independent confirmations (e.g., a SOC 2 type 2 certification).



Policy and Governance

Policy and governance are equally important. AI deployments should be reviewed against existing policies governing surveillance, data access, information security and acceptable technology use. Organizations may also need to establish new guidelines addressing AI-generated insights, human oversight, audit processes and accountability. While AI can automate analysis and surface insights, accountability ultimately remains with the organization.

Organizations should also establish a framework for evaluating risk versus reward. Like any emerging technology, AI introduces both opportunities and risks. The goal is not to eliminate risk entirely, but to understand it, manage it appropriately and determine whether the potential benefits justify the exposure.

Should you be using AI for investigations that may involve HR action or investigation, consider the creation of an AI-focused group or committee educated in all uses of AI in investigations (internal or external) and safeguards needed before any action such as apprehension, interview, accusation or prosecution.

Successful AI adoption requires more than technical performance. Organizations that address privacy, legal, policy, and governance considerations early are often better positioned to build trust, reduce risk and create sustainable long-term adoption strategies.

Final Thoughts & Key Takeaways

Artificial intelligence is no longer an emerging concept in retail security—it is already helping retailers reduce shrink, improve operational visibility and safeness, enhance customer experiences and make better informed decisions. The most successful deployments, however, are not necessarily the most advanced—they are the ones aligned to clear business objectives and supported by strong operational processes.

Throughout this paper, we've explored the differences between analytics, AI and generative AI. We've examined practical use cases currently deployed in retail environments and highlighted both the opportunities and limitations organizations should consider. While the technology continues to evolve rapidly (even as this paper is released) the theme remains constant: AI should be viewed as a tool to augment people, not replace them.

Retailers evaluating AI solutions should be focused less on marketing claims and more on measurable outcomes. The most valuable question is not "What is the latest AI can do?" but rather "What problem does it solve?" or "How will we measure success?"

The future of retail security will increasingly be shaped by intelligent systems capable of delivering greater visibility, faster response times and actionable insights. Organizations that approach AI with realistic expectations, clear objectives and a commitment to continuous improvement will be in the best possible position to capitalize from the benefits.

The question is no longer whether to utilize AI—it is "How can I learn to leverage it responsibly, effectively and in ways that create the most value for my organization?"

Key Takeaways for Retail Leadership

1. **Focus on business outcomes, not AI features.** The most successful AI deployments are the ones that solve a specific operational or loss prevention challenge.
2. **AI should help augment teams, not replace them.** Human judgment and verification are a critical step for investigations and response to an event.
3. **Competitive advantage comes from execution, not just adoption.** Simply deploying AI or a new analytic does not create value. Organizations that align that technology with people, processes and clear objectives will always see the greatest return on investment.



Key Takeaways for Integrators

1. **Become a strategic advisor, not just a technology provider or reseller.** Help retailers identify the right use cases for AI by understanding their operational goals, challenges and existing workflows.
2. **The greatest benefits come from connecting AI with video management systems, POS, smart LED or lighting, access control and other business systems.** AI is not a standalone solution.
3. **Camera placement, quality, infrastructure and user adoption all influence the success of any new system.** A successful deployment requires planning, ongoing maintenance and adjustments and continued customer education.



Key Takeaways for Suppliers

1. **Be transparent about capabilities, expectations and limitations.** Nothing can ruin a new project faster than disappointing outcomes from exaggerated capabilities.
2. **Demonstrate measurable business value.** Retailers are investing in outcome, not technology on its own. Show how your solution improves operations, reduces shrink, enhances employee and customer safety and increases efficiency with existing staff.
3. **Prioritize an integrated system.** Solutions that integrate with existing store technology have a much higher adoption rate than standalone solutions.



Key Takeaways for Corporate Stakeholders

1. **Help educate, not just advocate.** You know what the problems your store and management are facing more than anyone. Educate people on how a new integrated solution can make a positive impact on that specific problem.
2. **Crawl, walk, run.** Start slowly, even after success at one location. Make sure you can work out the kinks, hiccups or any other small issues before rolling out to more locations.
3. **Lead the conversation with facts, not hype.** Unfortunately, there is no miracle solution. Your store is unique, even if the problems you're facing are not. It's important to stick to facts on what this new solution can tackle, and your expectations if it's implemented. ■



SIA's Retail Security Advisory Board brings together retailers, security solution providers and technology leaders to collaborate on retail's most pressing security challenges, including AI in retail security, organized retail crime (ORC), data integration and technology adoption. With diverse members, the board provides a 360-degree perspective across strategy, operations, technology and risk management. Through thought leadership, best practices and topical papers, the group identifies high-impact industry challenges that require collective action, seeks to accelerate the adoption of innovative and effective security solutions and shapes practical recommendations and best practices for the retail security community.



securityindustry.org