Hanwha Vision

AI for Smarter Security:

A Guide to Enhancing Safety Through Technology

Jason Clement
Field Application Engineer Director
Hanwha Vision

Artificial intelligence, widely referred to as AI, is a broad range of technologies that enable computers to mimic human learning, decision-making, and problem-solving, allowing them to quickly perform tasks previously only achievable by (often time-consuming) human labor. AI can now process data, detect patterns and automate complex tasks for a wide variety of use cases.

In March 2025, Hanwha Vision America surveyed security and surveillance industry professionals to understand how they currently use AI and assess its use within the industry. Respondents included IT managers and executives, as well as security system evaluators, installers and administrators.

One thing is clear: the security and surveillance industry has widely adopted artificial intelligence, with 79% of users reporting increased reliance on AI in the past 12 months. We've used the survey results to inform this guide and have included some additional results on the following pages.

This guide covers the fundamentals of AI and security, including:

The State of AI in Security . . . 3
- Driving Innovation in Security and Surveillance . . . 3
- AI in Security . . . 4

Natural Language Processing . . . 4

Key Benefits of Edge-based AI . . . 6
- Edge Computing . . . 6
- Securing the Edge . . . 6

How is AI Being Used to Enhance Security Today? . . . 7

Real-time Event Notifications . . . 8

Benefits of Using AI to Enhance Security . . . 10

Implementing AI in Your Security System . . . 12

Compliance Considerations . . . 14

Real-World AI Applications . . . 15

The Future of AI in Security . . . 18

The Rise of Autonomous Security . . . 19

Case Studies . . . 20

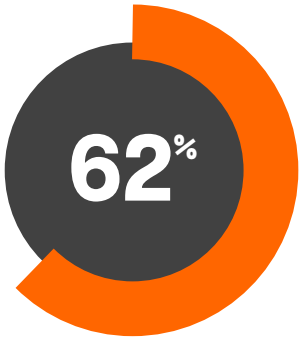
About Hanwha . . . 23

The State of AI in Security

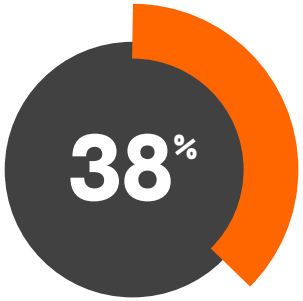
Artificial intelligence is revolutionizing modern technology, reshaping industries and impacting nearly every aspect of many organizations' operations. In security and surveillance, AI has moved beyond being a futuristic idea–it's here now and leveling-up industry best practices in significant ways.

Driving Innovation in Security and Surveillance

Over the past decade, AI has advanced from being available in only the most technically advanced applications to being widely adopted for household and consumer use. Today, AI has found its way into nearly everything we regularly interact with, including web searches, content generation, software and even household appliances. While the security industry certainly isn't unique in widely adopting AI, video surveillance already leverages some of the most advanced and exciting AI applications available – with more innovative use cases seemingly arriving daily.



of respondents say that their organization is utilizing AI daily in their security operations



of respondents say that they have already created custom AI security applications

An additional 29% say their organization plans to do so within the next 12 months

AI in Security

Smart security systems utilize surveillance video footage to generate actionable data, enabling more proactive monitoring and protection efforts. Security professionals are increasing efficiency and enhancing surveillance effectiveness by leveraging AI algorithms to assist in critical decision-making.

AI-based Object Detection

Security teams utilize data from AI object detection and attribute extraction running at the edge on the camera itself in real time. Local or cloud-based systems can also be used to access live streams from the cameras to perform even more advanced analysis, as well as scan archival footage.

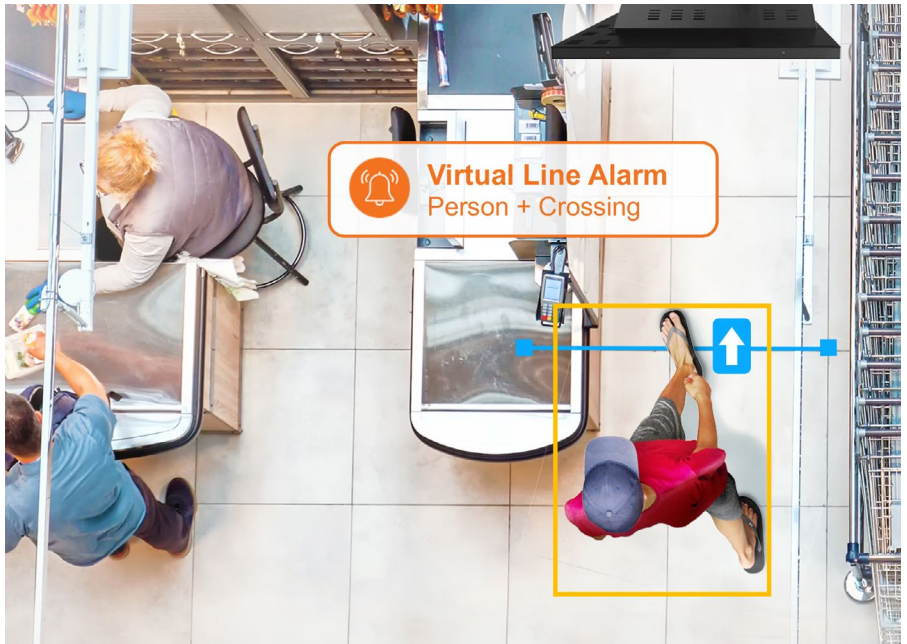
Additionally, AI-captured metadata enables security teams to access data on crowd dynamics, human behaviors and vehicular flow to detect irregular patterns that may indicate threats, such as aggressive behavior, theft, abandoned vehicles or other traffic anomalies in high-security zones.

False Alarm Reduction

Security professionals are deploying AI-enabled surveillance systems to help process and analyze massive amounts of video data in real time, filtering out irrelevant information to reduce the false alarms inherent in conventional cameras that use pixel-based motion detection. Automatically zeroing in on the most relevant data reduces user fatigue while increasing readiness and response times in threat situations.

Natural Language Processing

Natural Language Processing (NLP) is a branch of AI that enables software to read, interpret and respond to human language. In security operations, NLP-powered search tools can sift through large amounts of text, including security logs, threat-intel feeds and incident tickets, in seconds. By automatically highlighting suspicious patterns or keywords, these tools enable analysts to investigate and respond more quickly. Because the NLP models continually retrain on new data, their accuracy and usefulness improve over time, making the overall security workflow smarter and more efficient. These updates can be deployed via firmware updates for edge devices or software updates for software running locally. Cloud systems can update automatically, making it more straightforward to stay up to date with the latest technology.



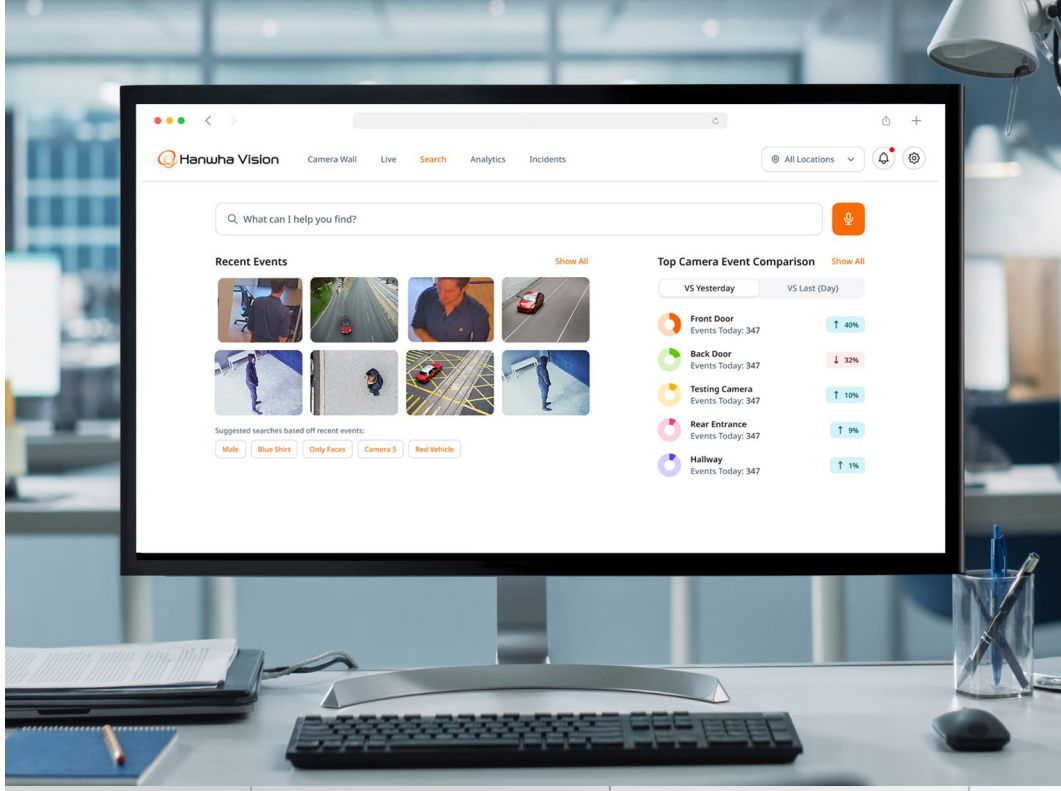
AI Search

Whether tracking a person, following a vehicle, or pinpointing unusual activity, AI-driven search delivers fast and accurate results, helping security teams respond more effectively and stay ahead of potential threats. AI search now includes smart filters based on object types and attributes – such as whether a detected object is a human or vehicle and its color, size or type – to enable security teams to zero in on key events in seconds, significantly reducing the time required to perform forensic searches. Automated tags, timestamps, and location information have made navigating massive amounts of footage far easier today than it was just a few years ago.

Audio Analytics

Advanced AI-powered audio analytics can automatically detect and identify the sounds of explosions, screams, breaking glass and more. Your AI-enabled devices can distinguish between routine sounds and potential threats and trigger real-time alerts when suspicious activity is detected. This technology is especially valuable in high-risk environments such as schools, banks and public spaces, where early detection can mean the difference between chaos and control. By improving threat recognition and reducing false alarms, AI-driven audio analytics make security more intelligent, faster and reliable.

Security teams gain immediate situational awareness, which leads to faster response times and more informed decision-making. Pairing AI audio analytics with video surveillance gives security teams a more complete picture – helping them better understand what's happening when they hear an alert.



Edge Computing

Edge computing enables AI models to run directly on devices, such as IP security cameras, at the “edge” of a network rather than relying on centralized on-premise devices or cloud servers. By processing data locally on the device itself, edge computing reduces latency, alleviates bandwidth constraints and helps reduce the total cost of ownership. Thanks to breakthroughs in edge computing, these security devices are now powerful enough to handle complex tasks that were once only possible with costly server infrastructure or cloud-based solutions.

Securing the Edge

Businesses deploying AI on the edge are taking proactive steps to enhance cybersecurity by isolating IoT devices, such as security cameras, from direct internet access, significantly reducing their vulnerability to attacks. Layered security strategies introduce multiple defense walls, making it harder for bad actors to breach systems and compromise sensitive information.

It’s important to use hardware that has received certifications from renowned independent organizations. A sampling of top-tier certifications includes:

- ETSI EN 303 645- Intended to prevent large-scale attacks against smart devices that cybersecurity experts frequently encounter by establishing a security baseline for connected consumer products and providing a basis for future IoT certification schemes..
- FIPS 140-3 - The latest version of the U.S. government computer security standard used to validate cryptographic modules, FIPS 140-3 aligns with the ISO/IEC 19790 standard and introduces several new enhancements to the security requirements relative to the FIPS 140-2 standard.
- SBOM (Software Bill of Materials) - Ensures that critical details of software components, such as version, name, license and functional description, are specified and managed, thereby enhancing security when using third-party and open-source code.

Key Benefits of Edge-based AI:

Cost Efficiency

- Avoid recurring cloud service fees
- Eliminate the need for costly specialized servers and AI-enabling software packages

Security and Privacy

- Enhance security and privacy by keeping sensitive data processing on-premises

Flexibility and Scalability

- Adopt Edge AI at your own pace or use it as a stepping stone toward hybrid solutions
- Support faster decision-making and reduce network dependency

How is AI Being Used to Enhance Security Today?

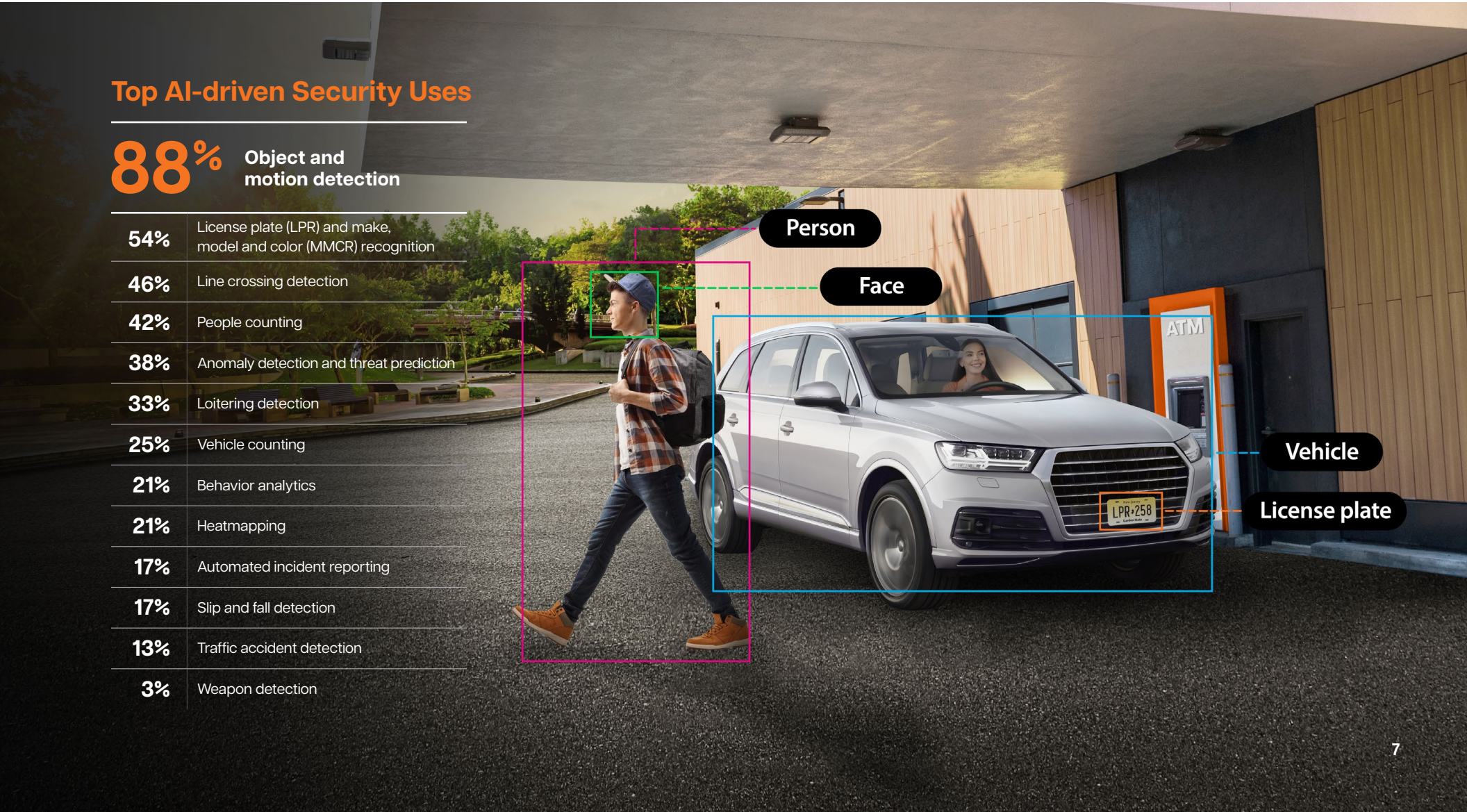
AI can be used with security cameras and video management systems to enhance security and access valuable insights for businesses in several industries.

Respondents to our survey are using AI in interesting ways. Object and motion detection, license plate recognition (LPR), line crossing detection and people counting are the most commonly utilized, with anomaly detection and loitering detection rounding out the top five use cases.

Top AI-driven Security Uses

88% **Object and motion detection**

54%	License plate (LPR) and make, model and color (MMCR) recognition
46%	Line crossing detection
42%	People counting
38%	Anomaly detection and threat prediction
33%	Loitering detection
25%	Vehicle counting
21%	Behavior analytics
21%	Heatmapping
17%	Automated incident reporting
17%	Slip and fall detection
13%	Traffic accident detection
3%	Weapon detection



Object Detection and Attribute Extraction

Security professionals utilize AI to automatically detect people, faces, vehicles, and license plates. Unlike traditional motion-based detection, intelligent algorithms can distinguish relevant objects and people from non-important background movements, such as animal or bird movement or a tree blowing in the wind, to reduce false alarms.

AI object detection captures searchable attributes, such as colors, carried or worn items, and more in security footage, helping them secure facilities and reduce time spent performing forensic searches. These models can accurately identify and classify objects of interest by analyzing real-time video feeds, even in low-light environments or situations with limited visibility.

In addition to streamlining investigations, AI enhances situational awareness, enabling faster decision-making and improving overall security operations. With continuous learning, AI models can adapt to new scenarios, ensuring they remain effective as circumstances evolve.

Re-Identification (Re-ID)

Re-ID matches an object across non-overlapping camera views, even when the subject leaves one scene and reappears in another. Powered by deep-learning models that extract fine-grained visual signatures (e.g., clothing textures, body shape, etc.), Re-ID systems convert each detection into a compact feature vector and then compare vectors frame-to-frame or against a gallery of past sightings. This lets operators trace a suspect's route through a facility, rapidly locate missing individuals or compile evidence packets without reviewing hours of footage.

Real-time Event Notifications

AI-enabled event notifications are replacing labor-intensive, repetitive tasks and improving response times. AI-enabled devices can automatically detect unusual activities or behaviors, such as loitering, trespassing or breaches of restricted areas. For example, an AI-enabled security system could trigger an alert to notify personnel that suspicious activity might be underway if an uncommon surge of customers were to occur at a retail store.

These systems can now understand standard movement patterns and trigger instant alerts when deviations from typical behavior occur. AI event notifications reduce reliance on manual real-time monitoring, allowing security personnel to focus on high-priority tasks and improving efficiency while minimizing the risk of missing key events.

Audio Classification

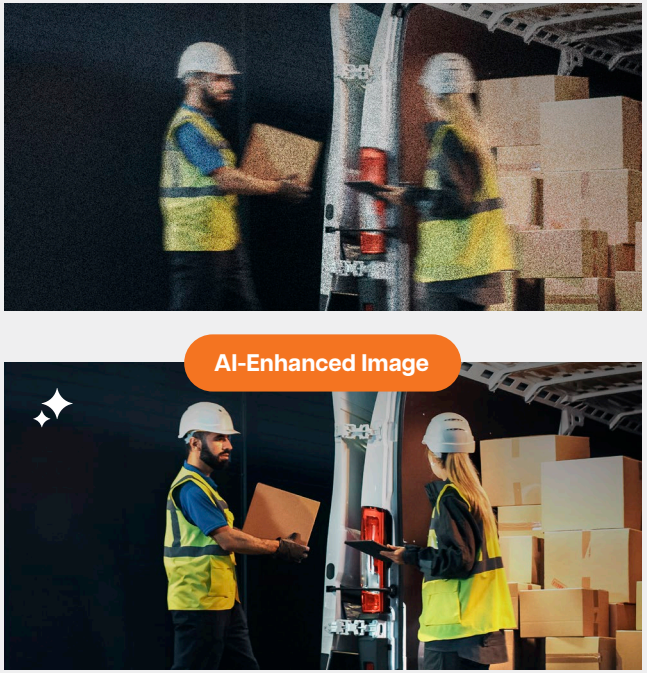
AI-powered audio classification actively monitors sounds in surveillance systems equipped with microphones, instantly identifying threats such as breaking glass or screams while preventing false alarms by ignoring irrelevant background noise. Security professionals can leverage AI to cross-reference live audio against a built-in database of high-risk sounds and immediately trigger an alert when it detects a precise match. They can then use this data to address hidden dangers – such as distant explosions or alarms – that video feeds might not capture.

Audio classification technology does not require recording, allowing for compliance with state audio laws. This dual-layer approach, which integrates audio analysis with video surveillance enhances threat detection and improves response times, thereby creating a more intelligent and proactive security system.

Image Optimization

AI is also used to enhance video quality and reduce storage bandwidth. Intelligent noise reduction, motion blur optimization and automated exposure adjustment ensure camera feeds capture critical details in all lighting conditions. With AI bandwidth reduction, security professionals can compress video feeds during idle times and enhance image quality when the system detects object movement to streamline footage storage.

AI-driven noise reduction eliminates random flickers and graininess in video before it's even compressed, ensuring the camera only sends real motion data instead of "fake" noise. That means each video frame takes up less space on the device and fewer bits to send over the network, saving both storage and bandwidth. Additionally, smart image tweaks, such as sharpening edges, balancing light and removing compression artifacts, make objects stand out more clearly to AI detectors. Together, these steps reduce file sizes, accelerate transmission and enhance the accuracy of your AI spotting tools, ensuring they work more effectively without missing or misreading any details.



Benefits of Using AI to Enhance Security

Implementing AI technology in an enterprise-level video surveillance system provides multiple organizational benefits, leading to a more precise, proactive and efficient approach to security.

Improved Surveillance

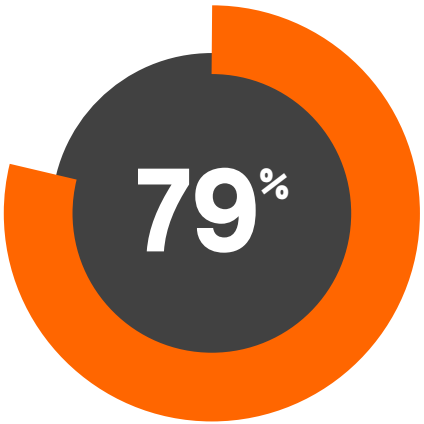
AI automates video processing, reducing the need for human intervention and minimizing the requirement for continuous system monitoring. AI can also analyze vast amounts of video footage in real time, detecting anomalies and critical events that require attention, ensuring that security teams can focus resources on strategic tasks. Moreover, AI-driven surveillance can process footage faster and, often, more accurately than human operators and offers superior detection capabilities in high-traffic and low-light conditions or scenarios where human resources are limited.

False Alarm Reduction

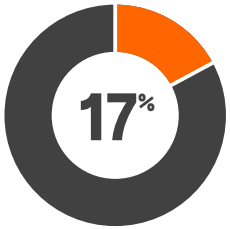
AI-based object detection surpasses traditional pixel-based motion detection by accurately distinguishing between genuine security threats and non-threatening events. Unlike conventional methods that may falsely identify moving trees or animals as threats, AI-based detection only triggers alarms if pre-determined objects or behaviors are detected, such as a person crossing a perimeter or a vehicle entering a restricted area. This precision reduces unnecessary disruptions, allowing security personnel to focus on genuine threats and improving overall efficiency.

Increased Forensic Search Efficiency

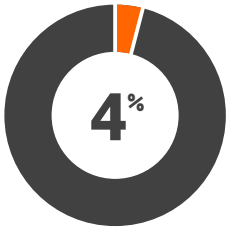
AI automatically detects objects and extracts detailed metadata, enabling security teams to rapidly locate footage based on the perceived attributes of a subject or suspect, such as a person wearing glasses, a hat, and a black shirt. AI saves all this metadata, enabling security personnel to easily recall relevant footage during forensic searches. The ability to use AI metadata to rapidly pinpoint a particular recorded subject, time, and location, rather than manually reviewing hours of footage, drastically reduces the effort required to investigate incidents, leading to faster response times.



of respondents report their organizations have increased reliance upon AI for their security operations in the last 12 months



same reliance



less reliance

Business Intelligence

AI-enabled business analytics include object counting, queue management and heat mapping, allows businesses to analyze their operations and take proactive measures to optimize efficiency. For example, AI can provide retailers with a visual map highlighting a store's busiest areas and times, providing insights on peak locations requiring additional staffing at certain times. It can also track the number of vehicles in a parking lot or detect long lines at service counters, enabling businesses to make data-driven decisions on resource allocation. These AI-enabled insights are helping companies better manage operations, improve customer experiences and predict future trends.

Custom AI Analytics

End users can also access and build custom analytics tailored to their specific use cases. By defining unique detection rules, behaviors or events, users can optimize operations to fit the needs of their environment. For example, manufacturers can train custom AI models to classify and count parts, as well as identify defects, as they pass through an assembly line, thereby automating production monitoring and quality control.

In addition to building analytics from scratch, users can download pre-built analytics packs that address common scenarios. These packs provide ready-to-deploy solutions for applications such as factories, retail and highways. This flexibility enables organizations to rapidly scale their security capabilities while maintaining the option to customize as their needs evolve. For example, pre-built worker safety AI packs can be deployed to recognize if objects are blocking a critical egress door in a manufacturing facility and send alerts to security personnel to remove the blockage, improving employee safety and avoiding hefty OSHA fines.

Implementing AI in Your Security System

While adding AI capabilities to security systems has never been easier, several barriers to entry have limited its widespread adoption. Cost, compliance concerns and lack of trust or understanding remain key obstacles for non-adopters.

Our survey found that the most common issues facing organizations were:

- **40%** Regulatory or compliance concerns
- **33%** Cost constraints
- **33%** Lack of trust in AI decision-making
- **27%** Limited understanding of AI capabilities

Despite these perceived constraints, implementing AI in a security system can now be accomplished with minimal hardware or software upgrades.

There are two low-barrier approaches organizations commonly take to ease into realizing the benefits of AI:

Install AI-enabled IP Cameras

The simplest way to introduce the power of AI into a video security ecosystem is through AI-enabled IP cameras. There is an AI-powered device designed to meet nearly any security use case – whether security teams are looking for dome cameras for discreet indoor monitoring, bullet cameras for long-range outdoor surveillance or multi-sensor cameras for full 360-degree coverage. These advanced cameras offer real-time event monitoring through AI object detection, attribution extraction, and even license plate recognition, providing critical insights that help security teams respond quickly to potential threats.

Many VMS platforms, including Wisenet WAVE, Milestone, and Genetec, are designed for seamless integration with AI-powered camera analytics, creating a unified security hub for managing and monitoring video feeds.

Advanced cameras offer real-time event monitoring through AI object detection and attribution extraction, and even license plate recognition, providing critical insights that help security teams respond quickly to potential threats.

Add AI to an Existing Camera System

Organizations that aren't ready or able to invest in cameras with onboard AI can enjoy many of the benefits of AI analytics by connecting traditional ONVIF cameras through AI appliances like the Hanwha Vision AI Analytics Box. These devices offer powerful data and actionable insights such as AI-enabled object detection and classification, motion detection, virtual line crossing and virtual area monitoring – without the cost or complexities of replacing an entire camera system. The AI Analytics Box integrates with several popular VMS systems, including Wisenet WAVE, Genetec and Milestone.

Compliance Considerations

Because AI-driven video surveillance converts routine video feeds into biometric data streams that can identify, track, and profile people in real time, regulators warn that covert or deceptive collection of faceprints, gait patterns or other “biometric information” can be an unfair practice. The U.S. Federal Trade Commission’s 2023 policy statement lists surreptitious facial analysis among activities that may violate Section 5 of the FTC Act if they mislead consumers or create undue risk. Europe’s new EU AI Act goes further, labeling the untargeted scraping of CCTV images for facial databases as an “unacceptable risk” and classifying most remote biometric identification in public spaces as “high-risk” AI, subject to stringent oversight.

Staying compliant requires more than installing cameras. Under the GDPR (and the UK GDPR), operators must choose a lawful basis — often “legitimate interests” or “public task” — carry out a Data Protection Impact Assessment, post clear signage, and store footage only as long as it remains “necessary and proportionate.” The AI Act imposes additional obligations for high-risk deployments: documented risk assessment, robust datasets, human oversight and accuracy testing before market release. In the U.S., state statutes fill the federal gap; Illinois’ Biometric Information Privacy Act (BIPA) prohibits the collection of facial templates without written consent, mandates retention schedules, and allows individuals to sue for violations. Together, these rules force organizations to incorporate transparency, consent, security and bias auditing into any AI-enabled surveillance project from the outset.

FEDERAL TRADE COMMISSION
PROTECTING AMERICA’S CONSUMERS

GDPR

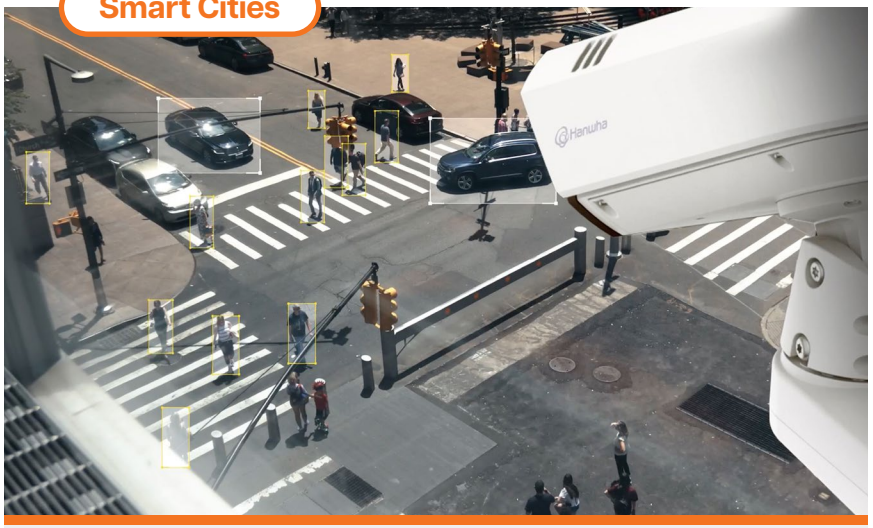
Illinois Biometric Information Privacy Act

EU Artificial Intelligence Act

Real-world AI Security Applications

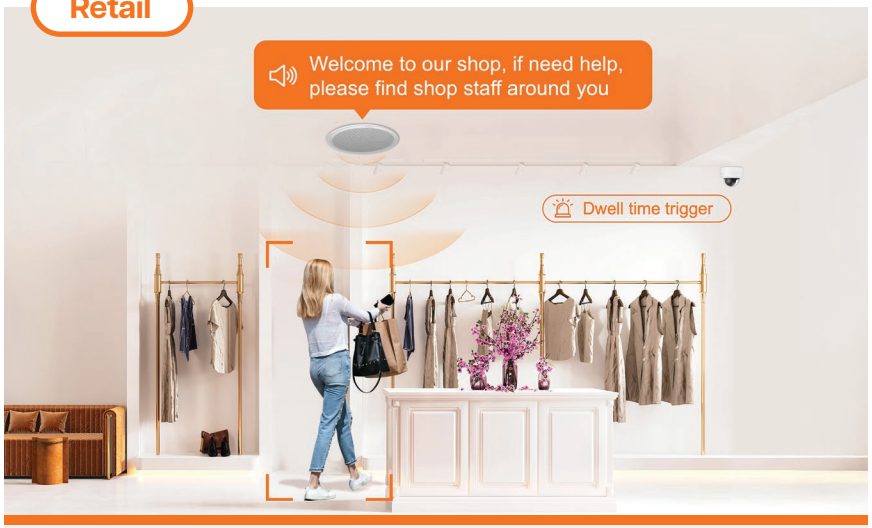
Countless AI use cases are happening in security right now across a wide range of industries, including:

Smart Cities



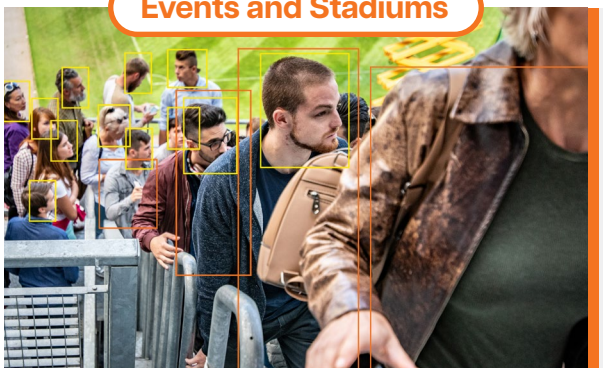
Video surveillance plays a crucial role in keeping today's cities running smoothly. AI-powered analytics make monitoring urban areas more efficient by recognizing license plates, detecting traffic violations, identifying break-ins or vandalism attempts and alerting authorities to antisocial or violent behavior. These intelligent systems also help manage public spaces by optimizing transit flow, deploying resources to prevent crowding and spotting road hazards like broken-down vehicles or spills. By providing real-time insights, these solutions enable cities to deploy resources more effectively and ultimately enhance the quality of life for citizens.

Retail



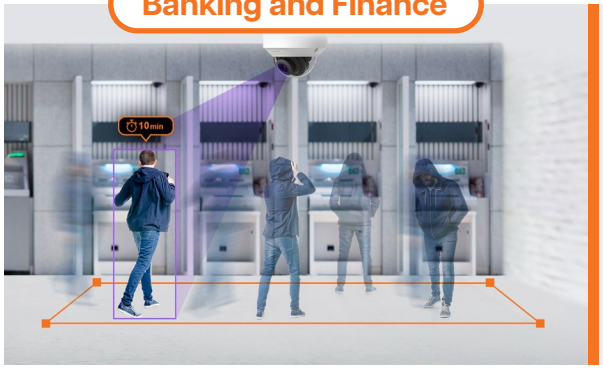
Intelligent video solutions do more for retailers than enhance security; they provide valuable business insights that drive sales, improve operations and create a seamless shopping experience. These advanced camera systems monitor everything from store entrances to aisles and stockrooms, using built-in analytics to help retailers optimize store layouts, refine product placement and manage queues in real time. By leveraging business intelligence tools like people counting, shopper tracking and visual heat maps to show popular areas of a store, retailers can understand how customers browse store sections, identify bottlenecks and make data-driven decisions to boost sales.

Events and Stadiums



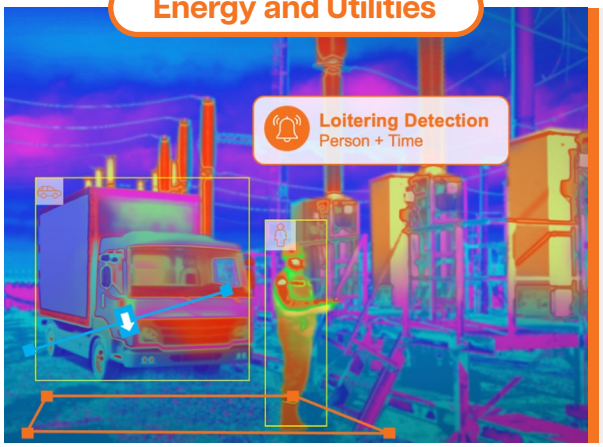
Modern security systems in stadiums and arenas leverage AI to keep visitors safe and enhance the fan experience. Security teams use high-performance cameras with AI-powered analytics to monitor everything from parking lots to seating areas to detect objects and trigger alerts when unruly or dangerous behavior occurs. Venue operators rely on AI-driven LPR to improve parking lot security while utilizing virtual line crossing and intrusion detection to help secure entry and exit points. Beyond security, these systems provide valuable business insights by tracking crowd movement and staff presence, generating alerts when long lines occur and offering insights to improve traffic flow.

Banking and Finance



Banking and financial institutions require specialized security solutions to protect assets and people. AI-powered analytics enhance security with features such as object detection, attribute tracking and perimeter crossing to proactively prevent theft and fraud, ensure regulatory compliance and build customer trust. Loitering analytics can be used to monitor vestibules and alert security personnel to suspicious activity. Discreet cameras with compact designs blend seamlessly into high-risk areas such as vaults, lobbies, teller counters, and ATMs for comprehensive surveillance. Banks can also gain valuable business insights by using people counting and heat mapping to track customer flow and optimize branch operations.

Energy and Utilities



High-risk environments, such as energy production facilities, critical infrastructure and utilities, benefit from AI-powered security systems in several ways. By utilizing object detection to secure perimeters and restricted areas, personnel can focus on more critical tasks, such as keeping critical equipment up and running. Specialized solutions – such as AI-powered thermal radiometric cameras – can detect abnormal temperature changes in equipment to prevent breakdowns or accidents. AI can also detect when personnel are not wearing PPE – hard hats, safety glasses, high viz apparel or gloves – in required areas and send automated warnings to those personnel or their managers. AI-enhanced surveillance solutions like these are helping protect vital public and private assets from security threats and safety hazards by enhancing situational awareness and ensuring operational continuity.

Corporate and Industrial Facilities

AI-driven video surveillance systems also enhance safety and operational efficiency in corporate and industrial facilities. With high-resolution cameras featuring AI-powered object detection to identify people and vehicles, security teams can improve incident response and reduce false alarms. Advanced LPR technology helps improve access control and incident tracking. AI-based analytics also enable intrusion detection, virtual line crossing, blocked exit and loitering detection to provide proactive security measures and ensure compliance with safety standards. Dynamic privacy masking (DPM) automatically obscures sensitive objects such as faces, vehicles and license plates to ensure compliance with privacy regulations without compromising security.

Manufacturing

Plant managers are using a variety of AI video capabilities to help optimize operations, enforce safety standards and reduce operational costs. Security teams rely on IP cameras and AI-enabled video management systems to identify incidents such as trespassing, failure to wear PPE, slip and fall incidents or equipment malfunctions and trigger notifications to allow safety personnel to intervene. Integrating AI into security systems for manufacturing also enables automated compliance management and equipment health monitoring to minimize downtime and maximize efficiency.

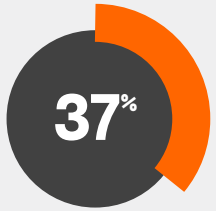
Cannabis

The cannabis industry utilizes AI to aid in a broad range of mission-critical tasks, from monitoring crop health to safeguarding customers and staff. AI analysis of video surveillance data keeps tabs on how crops respond to fertilizers and other treatments to help determine crop yields. Growers are using thermal cameras to identify the presence of damaging pests in growing areas. Keeping a long-term catalog of AI-searchable surveillance footage also helps growers maintain compliance with state regulations. On the retail side, detection of unauthorized entry or loitering, license plate recognition and people counting keep operations running safely and smoothly.

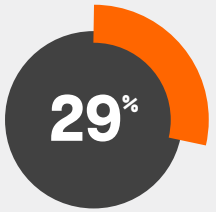
The Future of AI and Security

As artificial intelligence continues to evolve, the technology redefines how we protect people, assets and data, transforming security from a reactive necessity into a proactive powerhouse for businesses and municipalities.

Organizations continue to break new ground as they customize AI security applications for their unique needs and requirements. 37% of our survey respondents report that their organizations already use custom AI, and another 29% plan to implement customized AI applications within the next 12 months. We predict that custom applications will continue to grow across the industry over the next decade.

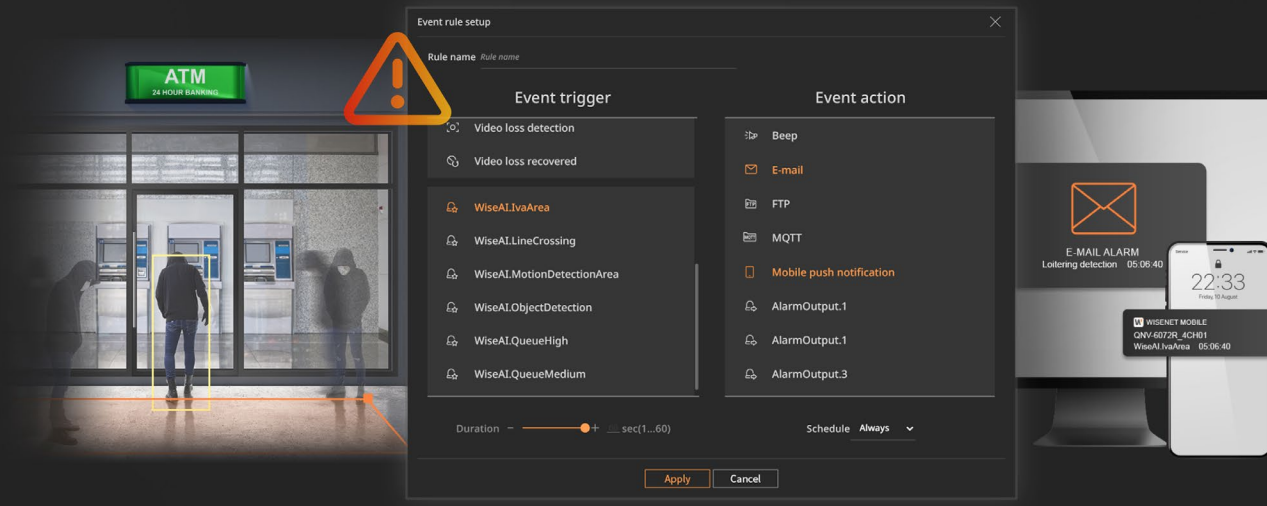


of respondents say their organization is already leveraging customized AI security applications

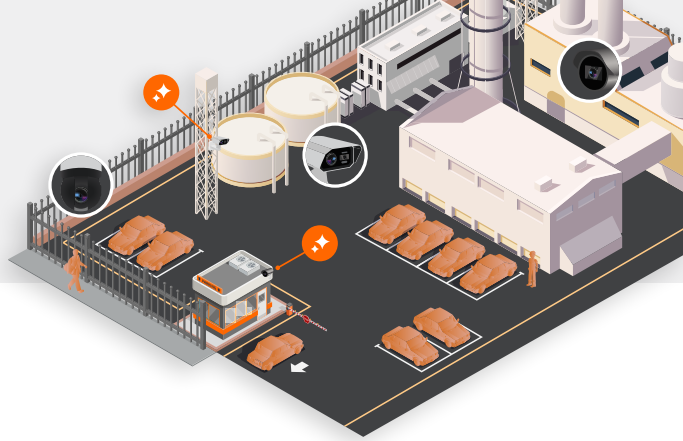


plan to implement custom AI in the next 12 months

By leveraging massive datasets and real-time analytics, AI can pinpoint potential threats with remarkable accuracy, anticipate security breaches before they happen and enable organizations to take action before an incident occurs. This shift from reactive to predictive security marks a game-changing evolution in how industries safeguard their operations.



The Rise of Autonomous Security



The demand for more intelligent, efficient solutions is increasing as security concerns evolve.

Soon, these technologies will integrate seamlessly into broader security frameworks, automating patrols, providing real-time monitoring and enabling immediate incident response. Drones, robots and intelligent platforms will extend security coverage, overcoming human limitations like fatigue and difficulty reaching hard-to-access areas.

As AI advances, autonomous technologies will become more sophisticated.. Smart city integrations could redefine urban security, enabling seamless coordination with existing infrastructure. Despite these advancements, human oversight will continue to be crucial. While autonomous systems improve efficiency, human judgment and ethics are irreplaceable and many situations will continue to require a personal touch.

One thing is clear, however: AI-enhanced security is here to stay and adoption is only increasing. Smart cameras and deep learning technologies will help drive the video analytics market to reach **$22.6 billion by 2028**[1]. Intelligent security systems are transforming asset protection by enhancing monitoring, patrolling and threat response capabilities without increasing staffing.

1. "Video Analytics Market Size, Statistics, Global Trends, Growth Opportunities and Forecast: MarketsandMarketsTM." MarketsandMarkets, www.marketsandmarkets.com/Market-Reports/intelligent-video-analytics-market-778.html. Accessed 4 Feb. 2025.

Case Studies

How organizations are leveraging AI for smarter security today

Sheriff's Office Uses LPR Cameras to Lock Down 360° Surveillance Coverage

With a capacity of 397 inmates from throughout Tennessee, the Dickson County Sheriff's Office facility needed intelligent video surveillance to monitor daily activity, eliminate blind spots and provide video evidence to state authorities.

When the office upgraded its surveillance system to Hanwha Vision cameras and a Wisenet WAVE video management system, Tim Eads, Sheriff, quickly realized that AI-enhanced image quality, movement tracking and license plate recognition (LPR) technology were game changers.

LPR cameras use AI to convert plates into machine-readable text and identify vehicle type, make, model, and color, allowing the department to track and detect all vehicles entering and exiting the property.

Hayes added, "With this LPR technology, we can set parameters. For example, if we are looking for a red truck, it will pull up vehicles with those features. We're usually recording all activity, and then when we need to pull up a specific incident or piece of footage, we can narrow it down at a later date and download specific video clips."

FULL CUSTOMER STORY HERE

"The system will detect stolen or wanted vehicles," Eads said. "If we have intel on a license plate, we can put that information into the system, and if that vehicle enters the parking lot, we get an alert."

Dwayne Hayes
Chief Jailer
Dickson County

Naval & Military Park Leverages AI to Preserve the Past and Secure the Future

The Buffalo and Erie County Naval & Military Park in Buffalo, N.Y., has a mission to honor all veterans, inspire appreciation for those protecting American freedoms and preserve the artifacts entrusted to the park's care. The extensive unfenced grounds, which allow public access to the property at any time, presented a key challenge as the park had experienced an uptick in vandalism.

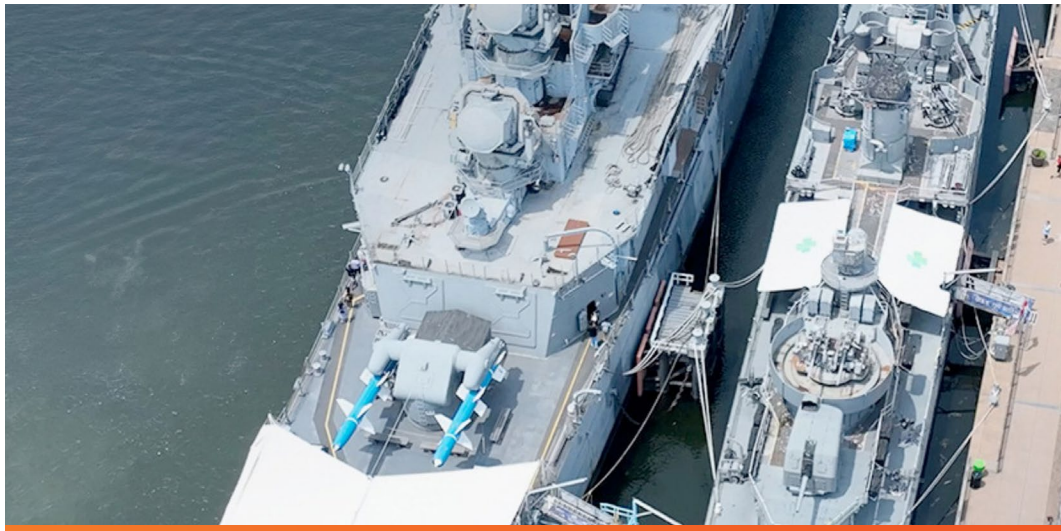
After installing multi-directional and AI-equipped cameras from Hanwha Vision, Director of Operations Bill Abbott says AI plays a key role in protecting the park while keeping the grounds accessible for visitors. While Hanhwa Vision 360° cameras cover a vast area around the park, AI uses object attribute data to make monitoring activity and finding footage after the fact easy.

Park security can now use the cameras to "positively identify someone who had done something, either damage or acts of violence," said Abbott. "You can use key identifiers, whether it's the color of someone's shirt, if they're wearing a backpack, or there's some physical feature that we can then go through and locate that person through the system," Abbott said.

"In the past, we had no capacity to effectively supply law enforcement with usable information to identify a suspect. We've changed that with the quality of cameras we're using."

Using AI to help identify the activities they would like to prevent has given the park's operations team a greater sense of security and control.

FULL CUSTOMER STORY HERE



> "In the past, we had no capacity to effectively supply law enforcement with usable information to identify a suspect. We've changed that with the quality of cameras we're using."
>
> **Bill Abbott**
> Director of Operations
> Hanwha Vision America

High School Uses Hanwha Vision Cameras in AI-Based Weapons Detection System

School security is deeply personal for South Pittsburg High School principal Tim Bible. As a former student of the school, Bible was a senior in 1985 when a student entered the school and shot a teacher.

Today, the school leverages Hanwha Vision digital IP-based cameras coupled with a first-of-its-kind AI weapons detection system from ZeroEyes to ensure the safety of its students and staff.

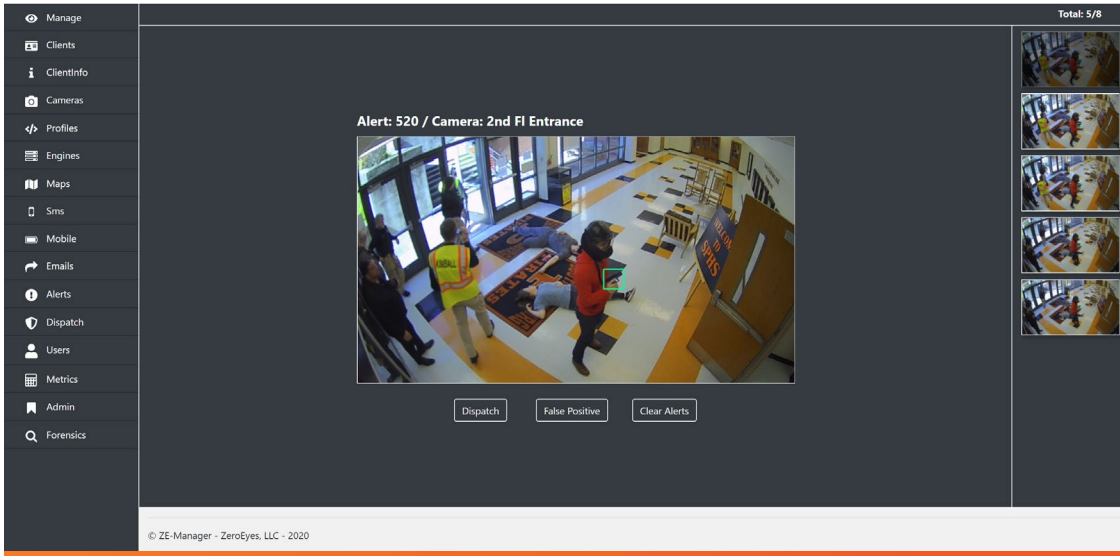
Hanwha Vision cameras, designed to capture the highest quality video footage in all lighting conditions, are located strategically around the school for maximum interior and exterior coverage. The ZeroEyes platform continuously analyzes this video footage, and its AI model – trained to recognize any type of gun – immediately alerts the ZeroEyes command center for analysis if a weapon is detected.

If credible, the system calls 911 to dispatch first responders and alerts the school resource officer (SRO), principal Bible, and other personnel on the notify list.

Being prepared for a school shooting is not an exercise that anyone enjoys, but it gives school principal Bible additional peace of mind.

“I’m looking at the cameras right now,” says Bible, and “the image quality coupled with a proactive solution to detect weapons, makes us truly feel that we’ve invested in the highest level of security to keep our students and staff safe.”

FULL CUSTOMER STORY HERE



> The image quality of the cameras, coupled with a proactive solution to detect weapons, makes us truly feel that we’ve invested in the highest level of security to keep our students and staff safe.
>
> **Tim Bible**
> South Pittsburg High School Principal

About Hanwha Vision

Part of the Hanwha Group, a Fortune Global 500 company, Hanwha Vision is a leader in video security solutions that offers a comprehensive line of security cameras, video management software and analytics that protect people, property, and data.

We are continually tailoring our portfolio of solutions to adapt to a changing security and surveillance industry. We're leveraging new AI applications in our devices to deliver precise detection, efficient bandwidth and robust search. Our growing ecosystem of cloud-based apps is enabling new on-premise and remote surveillance capabilities. These technologies, combined with our advanced business intelligence tools and AI-based data analytics, are helping organizations generate actionable insights to drive informed business decisions and keep people safe.

To learn more about how you can use AI to enhance your security systems, please contact us.

Hanwha Vision

© 2025 Hanwha Vision Co., Ltd. All rights reserved.

DESIGN AND SPECIFICATIONS ARE SUBJECT TO CHANGE WITHOUT NOTICE
Under no circumstances shall this document be reproduced, distributed or changed, partially or wholly, without formal authorization of Hanwha Vision Co., Ltd.