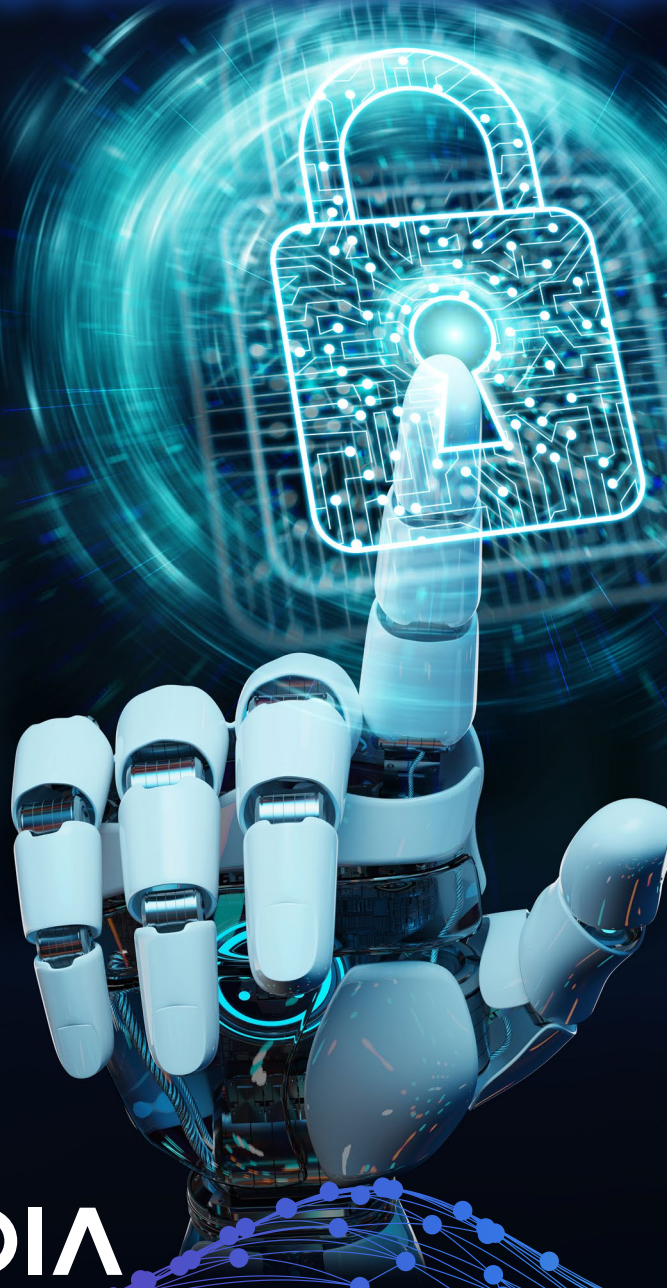


**Publication date:**  
April 2024

**Authors:**  
Scott Foley  
Niall Jenkins

# AI Outcomes in the Security Market and Beyond

Assessing the opportunity for systems integrators  
in security, operational, and marketing AI outcomes



OMDIA

intel®

# Contents

Introduction	3
AI and the installed base of video sensors	5
Future AI trends	7
Smart/safe cities	9
Retail	11
Sports and leisure	13
Manufacturing	15
Summary	17
Appendix	18

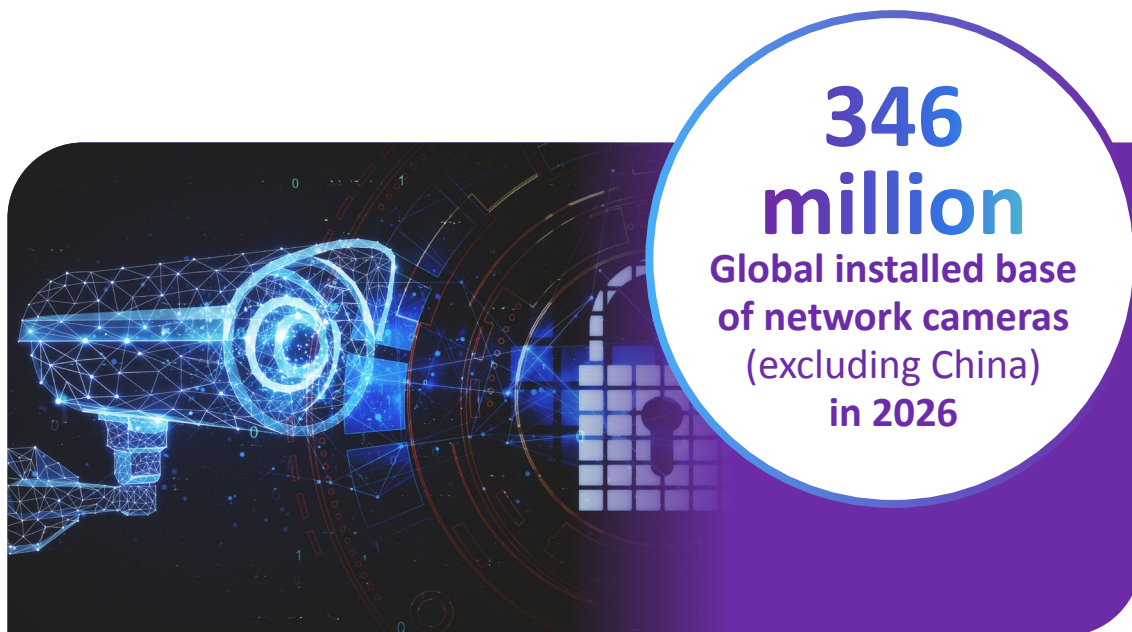


## Introduction

Artificial intelligence (AI) software is changing the way businesses and organizations operate across the consumer, automotive, industrial, and government markets. AI is a universal business opportunity for the technology industry.

In the video security market, network security cameras are the primary source of video images for AI and computer vision. However, the camera and traditional security use cases are only the start of the business opportunity. Outcomes for marketing, operations, sales, supply chain management, and people management functions can all leverage AI combined with existing video security infrastructure.

This is a critical opportunity for security systems integrators, solution providers, and other industry participants in the video security industry.



### AI market gains momentum

Video analytics have been an important part of the physical security sector for many decades, but with the evolution of AI based on deep learning analytics, these algorithms have become increasingly impactful over the last five years.

Thanks to improvements in processing capability, cameras and other edge devices have become powerful tools to run AI algorithms. This has opened the market to new solutions that require compute-intensive algorithms but benefit from the reduced latency of localized analysis and the reduced bandwidth requirements of edge processing.

At the same time, the physical security industry has also embraced cloud video or VSaaS (video surveillance as a service) architecture. The result is a best-of-breed approach to managing AI solutions. Some AI-based analytics are done on the camera, some in the cloud, and some with a hybrid combination of cloud and local processing. This transition will continue to gain momentum as processing power and algorithm capability develop.

## Moving beyond security

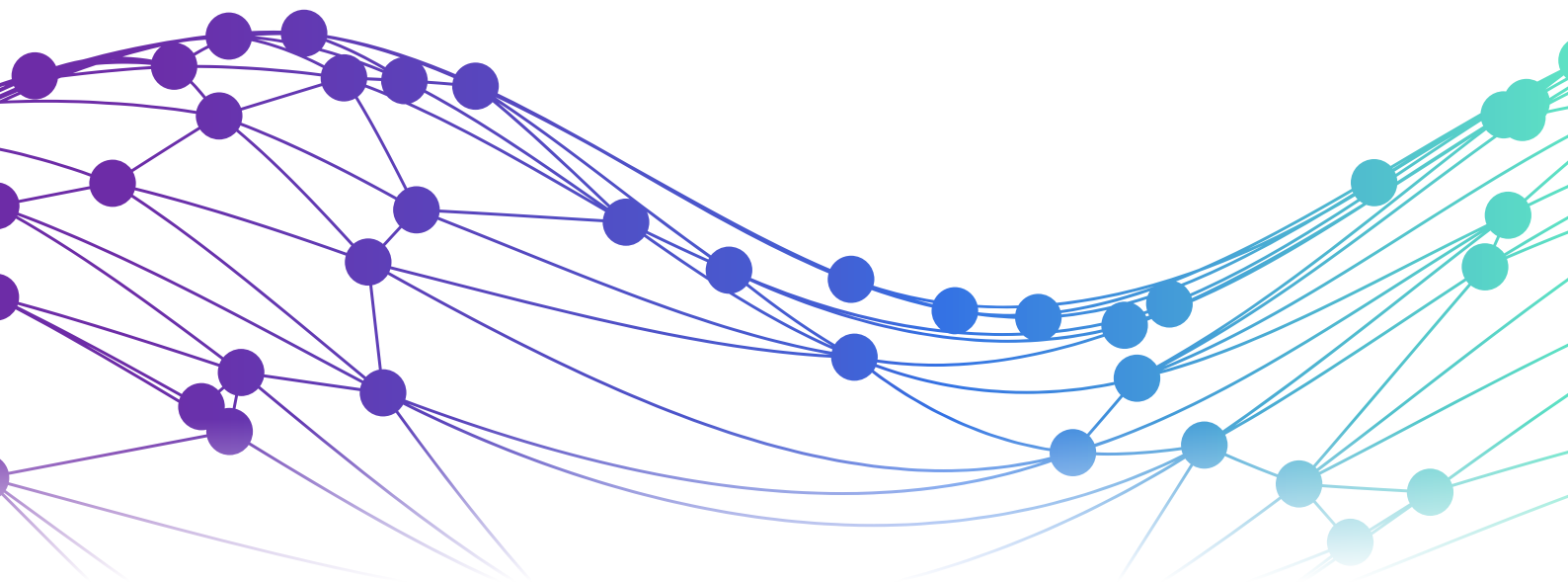
AI is now prevalent across many traditional physical security solutions. This includes perimeter protection and virtual tripwire, facial authentication, object detection and tracking, and behavior recognition. The next step in the AI journey will be to move beyond traditional security applications.

Leveraging the installed base of network security cameras—forecast to exceed 346 million by 2026—the security industry has an opportunity to take the lead in this already emerging AI market evolution.

Marketing, business intelligence, operations, and customer experience solutions can all be built on the video camera installed base. Additional sensors, such as AI-based sound analytics, can also provide inputs, whether that is detection of a gunshot or of an unusual noise in a manufacturing process that creates a predictive maintenance alert. In some cases, additional edge AI compute will be required to support these use cases. However, dedicated AI appliances or new servers can be easily integrated without affecting the already deployed infrastructure.

These steps do not need to be taken in one leap either. Many of the algorithms used in business intelligence analytics have components similar to those used in security applications. Service providers can learn how to apply new AI solutions in a phased approach, meeting the needs of new roles within existing clients, delivering similar algorithms in new applications, and steadily building a position in the operational processes of their customers.

This report aims to provide a background on the foundational security infrastructure on which the AI growth journey can be built. It will also analyze the key technology trends and the specific vertical roadmaps that can be used by security systems integrators and other security professionals to deliver successful AI outcomes.





## AI and the installed base of video sensors

Security integrators and other security service professionals are forecast to deploy an installed base of more than 346 million network cameras around the world (excluding China) by 2026. Each camera can act as a sensor input for an AI solution.

As network cameras become more affordable and the benefits become more widely known, the installed base is forecast to increase at double-digit growth rates. The transition away from analog cameras with the associated replacement opportunity is also driving market growth.

Many of the video analytics used in physical security started development in high-end, enterprise markets. Often, this meant a mission-critical system where budgets were readily available to support the development costs. People counting is a good example. These analytics have been used in crowd management applications in public safety for some time. Now, they are deployed in more cost-sensitive verticals such as retail and commercial. The combination of using existing video infrastructure, lower software development costs (the expense of initial development has already been incurred), less expensive compute power, better trained integrators, and the economies of scale of selling to larger markets means the overall cost of the analytics is lower. This has also resulted in traditionally high-end analytics being used in operational and business intelligence applications.

Figure 1: Installed base of network cameras by region, 2026

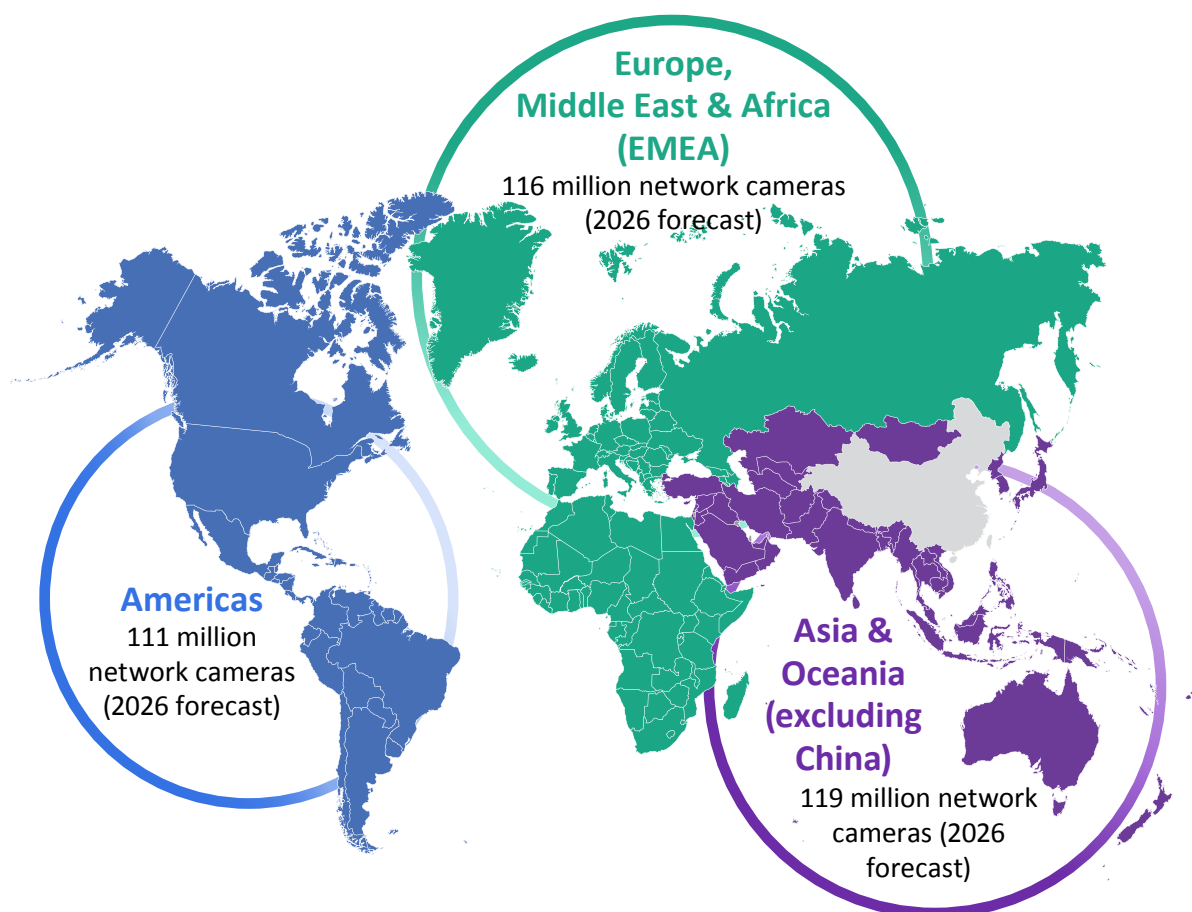
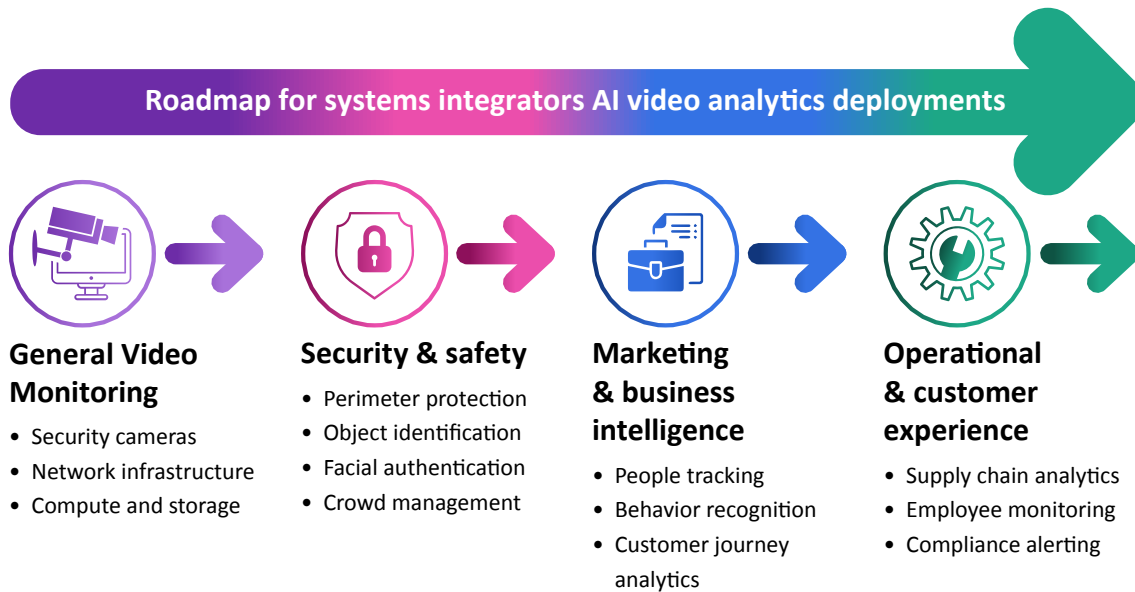


Figure 2: AI outcomes roadmap



Source: Omdia

© 2024 Omdia

The AI outcomes roadmap (see **Figure 2**) is likely to follow a similar path. In many verticals, there is a natural evolution. The first stage is the installation of general video security infrastructure. Security and safety analytics are then deployed by security professionals. The next step is to install object tracking or behavior analytics for marketing or business intelligence. These algorithms use similar infrastructure but often have new user roles and budgets within the customer. This could be the factory manager in the industrial market or the sales and commercial department at a retailer.

A key challenge is to develop new relationships within the end-user organization. In some cases, infrastructure costs can be shared across multiple client budgets, and often the engagement becomes more aligned to an operational benefit than to a perceived security cost. The IT department is another important stakeholder to engage in the process. It owns the internal network and is responsible for protecting infrastructure from cybersecurity threats.

The final stage in the AI roadmap involves AI outcomes that are embedded in the operational technology (OT) and solution. Applications can include supply chain management, compliance, and employee management. Solutions become ingrained in the end-user processes and evolve to be critical business processes. In some cases, AI solutions can be sold to a client's strategic partners.

Ultimately, AI will be pervasive across all industries and touch every part of the physical security market and beyond. Service providers and security practitioners that do not embrace this will end up missing a growth opportunity.

## Future AI trends

AI and computer vision outcomes will be built on the video sensors installed across the world. However, growth will be driven by the evolution in both software and hardware technologies.

### Software trends

The integration of AI with video, also known as computer vision, is increasing the edge processing capabilities for video security. Performant edge AI solutions mean real-time analytics are now possible on the network camera, whereas previously they were lower performance, slow, or only used in forensic (after the event) applications.

Furthermore, AI is providing new capabilities. It is broadening acceptance of and trust in automated response. Solutions can now combine AI for detection and analysis with the reliability and trust needed to initiate mitigating actions. It can integrate with other datasets, such as passive infrared (PIR) sensors or access control, to provide enhanced capabilities. In privacy, advances in federated learning models and differential privacy will allow video security access to more opportunities where analysis of sensitive data is less important than individual privacy.

AI solutions will also blur the lines between traditionally more separate applications such as security analytics, operational analytics, and business analytics. By integrating into the technologies above, such as predictive and remediation analytics and AI enhanced decision support systems, video analytics point solutions will cease to be siloed applications.

### Hardware trends

As AI software evolves, so do the computational power and resulting hardware requirements needed to support these outcomes. More powerful computing systems and specialized processors will become increasingly important.

Integration with edge devices will lead to increased investment in edge computing infrastructure. These devices will need to be designed with more diverse environments in mind, beyond the traditional data center. Energy efficiency will also become more important.

System architectures will need to emphasize scalability and flexibility and be able to scale up or down depending on real-time computational demand. Cloud computing will become more important to help with the requirement to scale and to backup local architecture. Hybrid architectures, offering the best of both cloud and edge processing, will also become more prevalent.

Advanced storage solutions will be similarly affected with new scalability and flexibility needs. Finally, higher power requirements, capabilities for handling advanced analytics, support for higher resolutions, and potentially longer operational durations will all have an impact on the hardware market.

An additional consideration with hardware will be optimization of software to maximize existing infrastructure. This includes AI optimization analytics toolkits for common platforms and simplified inference deployments of pretrained models. Designing the software with the hardware platform in mind can reduce the need for more expensive specialty AI solutions.

## Market trends

Computer vision trends in other industries have the potential to affect security professionals. For example, generative AI advancements could make data training easier to produce and use. Segments that share computer vision needs such as smart cities, smart buildings, automotive, and retail are investing heavily, and outcomes will evolve quickly.

Some examples include advanced neural networks and 3D imaging/LiDAR in autonomous driving, edge computing and facial identification in smart city infrastructure, motion detection and tracking in sport analytics, and gesture recognition in retail and gaming. These evolutions could make keeping pace with the technology more difficult. However, security professionals that keep pace, expand, or specialize in these developments will find themselves ahead of their competition and will be early thought leaders.

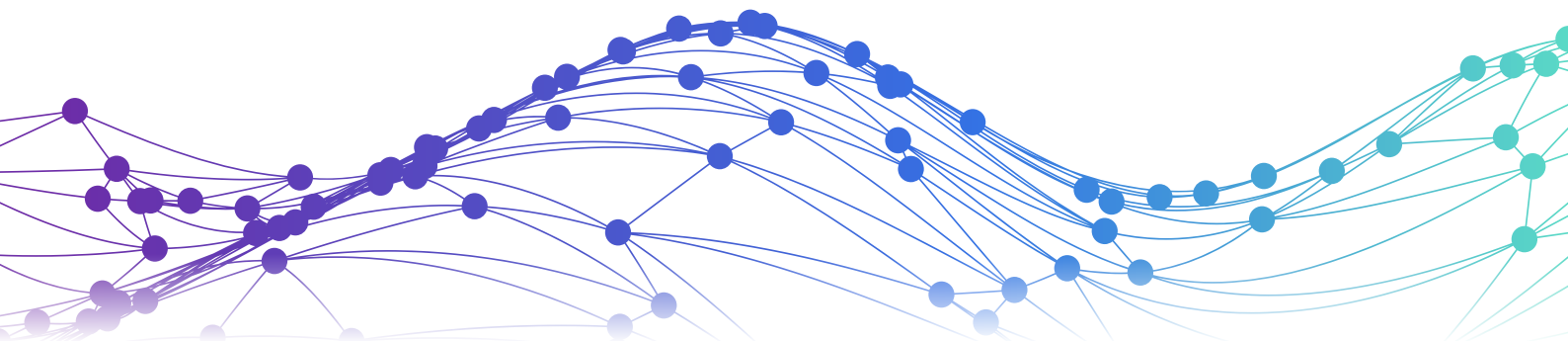
Similarly, security professionals will increasingly need a foundational understanding of AI principles, machine learning algorithms, and their applications. This requirement could extend to an ability to manage large volumes of data and the skills to extract insights from or beyond current analytics offerings.

Cybersecurity is another area of focus. Ensuring that physical security and cybersecurity requirements are considered together is important because one cannot exist successfully without the other. This also requires skilled people that understand the role of cybersecurity in the overall security of an AI solution. As cyberthreats continue to evolve this role will be increasingly important.

Finally, the cost and complexity of AI outcomes is still high. Enterprises may not find this daunting, but many smaller organizations will continue to use less expensive solutions that have a wide range of installers and can be maintained efficiently. Legacy systems can be difficult to displace in the security industry.

Consequently, the benefits and opportunities inherent in AI must be promoted and justified. At this point the market is still relatively young. Manufacturers, integrators, and third-party institutions have an opportunity to display leadership and provide a mentoring role. The rest of the industry will have to invest in training or expand hiring areas to accommodate this in the future. Showing how AI can be applied across different end-user industries will form part of the growth story.

The following sections provide a deep dive into four vertical markets and the AI outcomes that will shape these industries in the future.





## Smart/safe cities

A smart city can be defined as an urban environment enabled through the integration of technology that leverages data and digital infrastructures to improve quality of life and overcome existing or anticipated challenges in the city.

Public safety and security applications, often referred to as safe cities, are one component of the smart city. Another is mobility and transportation, which includes smart parking, ticketing, and traffic management. A core technology in these systems is the installed base of security cameras.

The smart cities market globally (excluding China) has almost 30 million network cameras installed. Most of these cameras are deployed in city surveillance applications. Cameras typically deal with complex scenes and variable environmental conditions, which can be a barrier to deploying video analytics solutions. However, these systems are also mission critical, and significant budgets are available to support more advanced AI outcomes.

AI is well suited to mitigating some of the challenges faced by the city managers and police departments responsible for public safety. Managing crowds in city centers is one such challenge. Police departments need to understand when an event escalates to the point where first responders are required to intervene.

City leaders also need systems that can provide vigilance. This could be in the form of an alert to vandalism or unauthorized access to a secure location. Finally, video analytics can also help in forensic search applications to increase the speed of an investigation.



### Smart/ safe cities

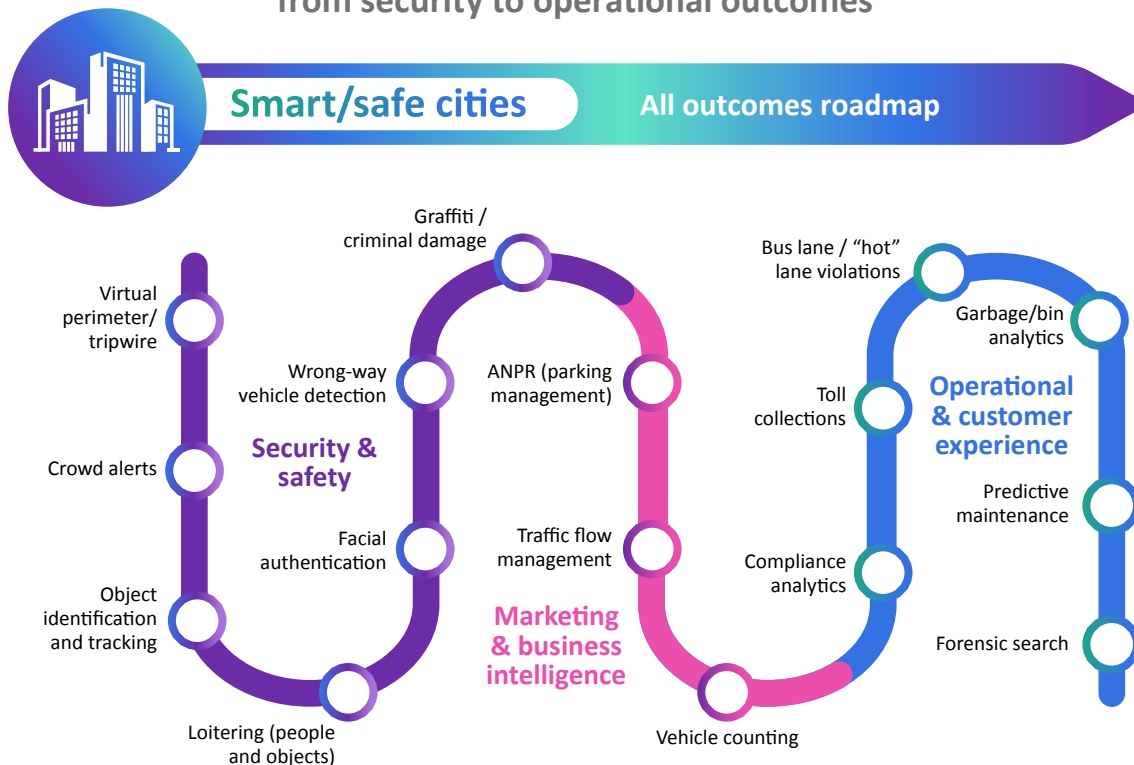
**29.4 million sensors  
forecast in 2026  
(global, excluding  
China)**



### AI outcome roadmap

Security and safety applications are at the core of the video analytics deployed in the smart and safe city. End users and decision makers are often led by police departments and city leaders who want to ensure that their citizens feel safe living in the city. Consequently, the AI outcome roadmap starts with many traditional public safety applications. Video analytics include perimeter detection, crowd alerts, public nuisance alerts, and object detection and tracking applications used to protect both people and infrastructure. In some regions, facial authentication algorithms have gained market share. However, barriers to deployment remain, especially around privacy and how to manage and store personal information.

**Figure 3: Smart/safe cities: AI outcomes roadmap from security to operational outcomes**



Source: Omdia

© 2024 Omdia

In many of the vertical market AI roadmaps, there is not always a clear point where an application moves from one outcome type to another. Wrong-way detection is an example of an application that provides a security and safety outcome. It creates an alert when a vehicle travels the wrong way down a road. However, it can also provide a business intelligence outcome that supports traffic flow analysis and the increased efficiency of city operations.

Vehicle counting is another business intelligence solution that city leaders can use to manage the road network. Automatic number plate recognition (ANPR) analytics or license plate recognition (LPR) can also be used to identify which specific vehicles are parked incorrectly. Similarly, there is some overlap in use case with bus lane and "hot" lane violation analytics, which can identify a vehicle in an incorrect road location and issue a ticket based on the LPR identification. These could be considered operational analytics.

Compliance analytics have increased in value since the coronavirus pandemic. Here, analytics can identify when people are too close together and potentially spreading the virus. It can also identify when individuals are not wearing masks. Predictive maintenance of outdoor locations is another operational solution. Video analytics can be used to identify potentially damaging items that could break escalators or other infrastructure. Sound analytics could also be used to provide alerts to unusual operational sounds that could imply some maintenance is required.

Finally, forensic search is a valuable AI outcome for city surveillance solutions. Searchable analytics work by creating a metadata stream in parallel with the video stream. This metadata stream acts like an index or list of contents. When there is an event, key information such as the size, color, object type, speed, event time, and duration are stored in the metadata stream. This metadata can then be searched independently of the video. In a police investigation, this has the potential to save significant investigation time.

## Retail

Retail can be a difficult market for the application of physical security solutions. Customers have access to most locations in a store, at least during opening hours, which makes securing a perimeter difficult. Any equipment installed must also be discreet so as not to reduce sales. While this trend has limited impact on computer vision and security cameras, it can affect other security equipment such as physical barriers, access control and intrusion detection.

Retail is also an industry in transition. Sales are moving to e-commerce, reducing the need for store locations. This transition has accelerated following the coronavirus pandemic as customers become more open to online purchasing. Additionally, there has been an uptick in theft and loss from stores in some regions. Budget can also be a challenge in an industry that historically had limited margins.

Despite these challenges, the retail market globally (excluding China) has more than 41 million network cameras installed. This is a huge installed base of video sensors ready to support AI outcomes. It also has many challenges that can be improved by AI.

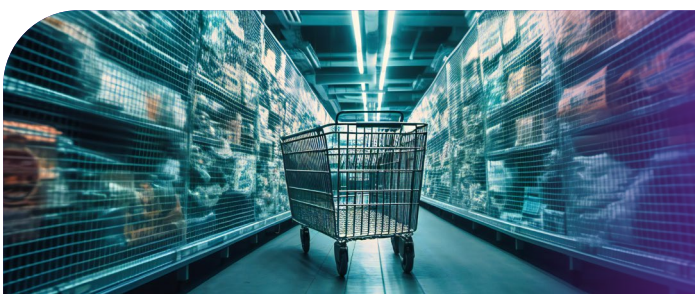
These opportunities are as diverse as physical security and loss prevention solutions, business intelligence, and operational outcomes. There is also growth potential. Most of the retailers that have deployed video analytics or computer vision solutions are larger, enterprise retailers. Larger organizations benefit from the scale of deployments, typically starting with a few locations and then rolling out to their wider base of stores. They also have the funding to support these installations.

The longer-term opportunity will move to the small-to-medium-sized businesses that can capitalize on the lessons learned at the enterprise level to support their security and operational requirements.



### Retail

**41.1 million sensors  
forecast in 2026  
(global, excluding  
China)**



### AI outcome roadmap

Loss prevention is a primary challenge in physical retail stores. Analytics such as object tracking, people tracking, and behavior recognition all have a role in helping security guards to manage the threat of theft. In some geographic locations, facial authentication has also been implemented to identify bad actors before they enter a main store location. Video security and video analytics have a particularly important role in the security system because of the inherent challenges of physical infrastructure to protect products and staff. In addition to staff protection, other safety analytics can be installed. Slip and fall analytics can recognize that someone has had an accident and alert a member of staff to come to their aid. It can also provide evidence in the case of any legal challenge from the customer over their safety.

AI is well suited to supporting the marketing and business intelligence requirements of a retailer. People-counting analytics can be used to track conversion rates between people entering the store and people purchasing an item. Heatmapping can provide insight into the areas of the store where customers spend most of their time. Dwell-time analytics can provide insight into how long they spend in these locations and can support more operational solutions such as queue management alerts when too many customers are waiting for a checkout.

Further along the value chain, customer journey solutions can help retailers to understand more about their customers by providing analytics and data to support marketing and product decisions. Supply chain management can also benefit from AI. Recognizing that a product is no longer on a shelf can help retailers to both restock the shelf and order new products more efficiently. There are also examples where retailers have implemented similar analytics solutions down their supply chain to help integrate their solution with a partner.

Finally, autonomous stores and self-checkout management are increasingly strategic in the retail business plan. Some of the infrastructure installed during the pandemic is helping. Additional security cameras were needed to provide oversight when retailers had lower staff numbers. Now, the additional capacity these infrastructure investments have provided forms a good basis for AI outcomes to build on.

One consideration that arises as retailers look to deploy more AI outcomes into their stores is what this does to the physical infrastructure requirements. Ensuring that the power and compute level is high enough to manage these requirements is an important step in mitigating any challenge once the solution is operational. Integrators also need to engage with people from the data science and data engineering staff and those from lines of business such as chief revenue officer and chief marketing officer.

**Figure 4: Retail: AI outcomes roadmap from security to operational outcomes**





## Sports and leisure

The sports and leisure sector is the smallest sensor installed base of the four vertical markets addressed in this white paper. It includes all facilities where sporting events and leisure activities take place, including sports stadiums, fitness centers, and public swimming pools. Though it may lack the scale of the smart cities and retail markets, it does represent an interesting and diverse AI market opportunity.

Large sports stadiums must deal with many of the challenges relevant to other vertical markets. Merchandizing stores and food courts require retail applications. There are crowd management and ticketing challenges. Parking management is also in scope as an operational application. Finally, computer vision can be integrated into the broadcast experience to bring new features to the viewer watching on TV at home.



### AI outcome roadmap

For systems integrators active in the sports and leisure market, many of the analytics opportunities have been in traditional security applications. These include virtual tripwire alerts used to protect higher-value locations that are off-limits to the paying customer. These algorithms can also be used when the location is not in operation to provide a perimeter security application.

Another security application that is relevant is loitering alerts. When a person or an item, such as a bag, has been in one location for a predefined period, an alert can be sent to a security guard to check out the situation. Augmenting guarding is a security efficiency outcome. Similarly, blocked-exit applications can recognize that a security exit is blocked and send someone to deal with it. With the scale of many stadiums, it is important that people can exit the location in a safe manner in the event of an emergency.



**Figure 5: Sports and leisure: AI outcomes roadmap from security to operational outcomes**



Source: Omdia

© 2024 Omdia

In terms of marketing and business intelligence analytics, people-counting, and dwell-time solutions are well suited too. They can provide many of the same benefits that these analytics provide in the retail market, helping to manage location population and providing business intelligence to retailers within the stadium.

Operational applications include parking management, crowd management, ticketless entry, and digital-signage integration. Furthermore, some of these applications can be integrated. For example, depending on how busy a location is, signage can be used to send people to different exits or to ask them to wait for a short period before making their exit.

Digital twins are another emerging opportunity. Network security cameras can help to build up a digital picture of the sports stadium. Once this is built, different procedures can be modeled to review what impact they would have on operations. Though this approach is a long way from the traditional security and safety outcomes that most systems integrators are familiar with, it does show the potential opportunity to integrate systems in the sports and leisure market. Likewise, the deployment of enhanced experiences using broadcast video sensors is another longer-term opportunity for security professionals.

## Manufacturing

A key trend in the manufacturing sector is the digitalization of the industry and convergence of IT and OT (including security cameras). As the market moves to more efficient operations, there has been increased acceptance of cloud, a focus on digital twins, and an increased need for integration and management services. Many of these trends will support manufacturing AI outcomes across business intelligence and operational solutions.

The manufacturing sector includes all facilities involved in the production of goods. Some of the subsectors that make up this category are automotive, chemicals, farming and agriculture, food, pharmaceuticals, textiles, metals, paper, and machinery production. It is forecast to account for an installed base of more than 24 million cameras (excluding China) in 2026.

Manufacturing end users are typically interested in increasing productivity, ensuring employee safety, and managing the quality of their supply line. Consequently, security integrators that can tap into these focus areas with AI solutions should grow their business and develop better, long-term relationships with the manufacturing end user.



### Manufacturing

**24.3 million sensors  
forecast in 2026  
(global, excluding  
China)**



### AI outcome roadmap

The manufacturing sector offers a more controlled environment than the other vertical markets assessed in this report. The perimeter is protected, physical access control equipment supports entry management, and there is a lower chance of external bad actors gaining access to the main building.

As a result, the security and safety video analytics sold in the manufacturing market are different from those found in more open locations. Video-based fire analytics can provide alerts when smoke is detected. Virtual safety curtains can turn off machines when someone breaks the barrier created by the analytics. Evacuation management systems can track the number of people on site and ensure that everyone gets out of the facility in the event of a threat.

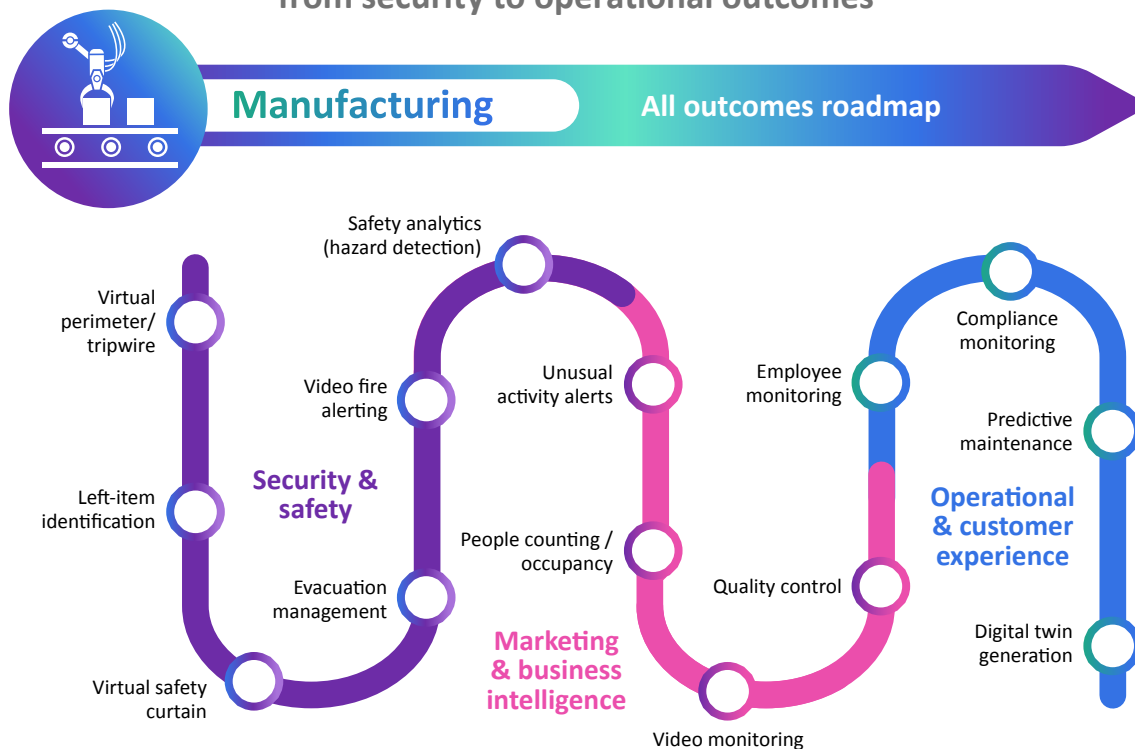
Business intelligence solutions start to move into people-counting and video-monitoring solutions. These support some of the decision-making that manufacturers need to do to ensure they support their priorities of productivity, safety, and quality.

Quality control is an important element of the AI roadmap. These solutions can be involved in the identification of when threshold limits are exceeded in a manufacturing process and in the application of deep learning for image inspection, often referred to as machine vision. Events-based imaging is an emerging sector in manufacturing that provides a constant stream of data capturing location data missed by traditional static images. Video streaming is also increasingly popular among manufacturing end users.

Operationally, compliance monitoring can support monitoring of the use of safety gear and the manufacturing process. Predictive maintenance is another key AI outcome. Productivity is a core focus area, and any solution that improves it is valuable. An additional integration with sound analytics, to alert to unusual noises from the machinery, can add another layer of mitigation.

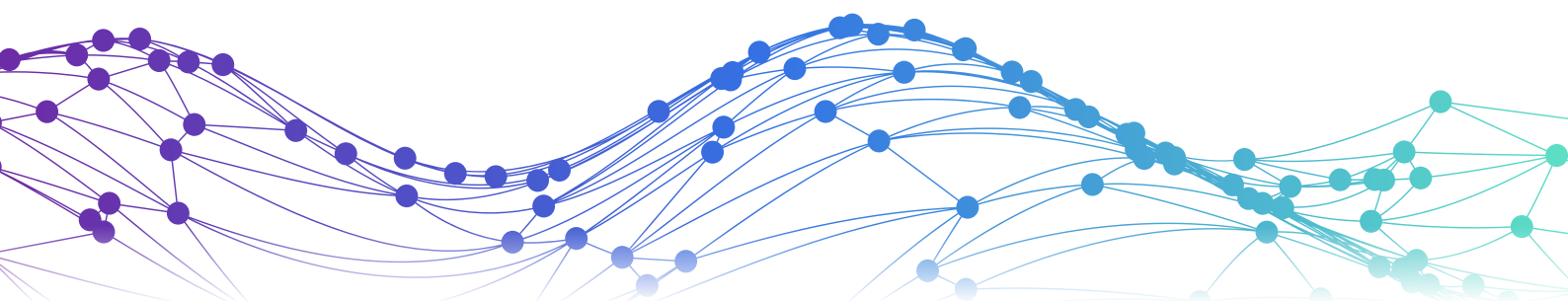
Finally, digital twins are increasingly important tools that can help with quality management. Their purpose is to predict, simulate, optimize, and capture real-time performance data for analysis. Digital twins can also remove the need for prototyping, reducing waste from materials that would otherwise be used. AI outcomes that support the generation of digital twins can therefore help to improve sustainability and reduce costs.

**Figure 6: Manufacturing: AI outcomes roadmap from security to operational outcomes**



## Summary

- **Security integrators and other security service professionals are forecast to deploy an installed base of more than 346 million network cameras around the world (excluding China) by 2026.** Each camera can act as a sensor input for an AI outcome.
- **Computer vision is increasing the edge processing capabilities for video security.** It is also accelerating the pace at which video data is interpreted in real time versus postprocessing applications.
- **Smart city end users are looking at operational or business intelligence outcomes.** Video analytics that support traffic management and parking violation or toll ticketing can produce a revenue stream. AI outcomes can support cities in managing operational challenges.
- **Security analytics deployed in the retail market have been successful.** However, engaging with only the loss prevention and security leaders at a retailer will limit the growth opportunity. Increasingly, operational and customer experience analytics are gaining mind share. These applications can make a strategic difference, such as ensuring a more efficient supply chain, reducing the cost of operations, or supporting more product availability. One challenge is bringing the disparate roles within the retailer to the same table.
- **The sports and leisure market is an interesting opportunity for security integrators.** Many of the security analytics relevant in other verticals are equally relevant to these end users. The projects are also high value and high profile. Partnerships will likely be required, at least initially, for more operational and customer experience outcomes.
- **The manufacturing market represents a different opportunity.** Many of the security and safety AI outcomes support one of the core objectives of a manufacturing end user, which is primarily to ensure the safety of its staff. Operationally, security cameras can reinforce process compliance and quality management and even help in the creation of digital twins. As integrators travel along the AI outcomes roadmap, they will add value to their manufacturing end users. This should also open new budgets and customer roles with the manufacturing sector.
- **The AI outcome roadmap does not need to be followed in one leap.** Systems integrators can expand their offerings from security and safety analytics through marketing and operational outcomes. This transition shifts a solution from a security cost to a safety, productivity, or revenue-generating outcome. It also supports better customer relationships and should drive market growth opportunities in the future.



# Appendix

## Authors

### Scott Foley

Senior Analyst, Physical Security

### Niall Jenkins

Consultant, Physical Security & Building Technology

## Get in touch

[www.ondia.com](http://www.ondia.com) | [askananalyst@ondia.com](mailto:askananalyst@ondia.com)





# Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision-makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantages for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

## Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") or its third party data providers and represent data, research, opinions, or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.

