



Guide

The power of AI in modern security

Discover how advancements in machine learning, edge processing and predictive analytics are advancing AI-powered security solutions and enabling organizations to have a more proactive security posture.



The power of AI in modern security operations

Security technology generates vast amounts of data—from video footage and access control logs to audio analytics and sensor inputs. Managing and making sense of this data in a timely manner is the biggest challenge for many security teams. Traditional, manual processes are no match for the volume of data security teams deal with today.

But imagine if you had a system that could instantly analyze countless hours of video or know who should be where and when—freeing up your security team to focus on verifying real threats instead of sifting through endless streams of information and alerts. This is the promise of AI-powered security solutions.

Although generative AI tools have recently brought AI into the spotlight, AI has long been used in physical security technologies to make sense of large amounts of data and distill it into actionable insights. The impact of AI on physical security is twofold: it improves the efficiency of security teams by focusing attention on real threats and reducing missed incidents, which in turn enables quicker and more effective response.

This guide offers an in-depth look at the latest AI trends in physical security, covering advancements in machine learning capabilities, move to edge processing and the advancement of predictive analytics. You will learn how AI-driven analytics and object detection are augmenting security operations by automating routine tasks, improving threat detection and enabling more proactive responses. By the end, you will have a clear understanding of how AI-driven solutions can enhance your organization's security posture and support human-led decision-making.





AI trends in physical security

Today's safety challenges demand the latest technology. Advancements in AI, along with machine learning, cloud computing and data storage infrastructure, have enabled faster and more accurate threat detection, allowing organizations to adopt a more proactive security posture.

These are the most notable trends in the adoption of AI technologies in physical security:

Advancements in machine learning algorithms

Recent advancements in machine learning algorithms have significantly expanded the capabilities of AI in security systems. The development of sophisticated neural network models, particularly advanced convolutional neural networks (CNNs) and transformers, has improved object detection, facial recognition and behavior analysis capabilities in video security systems. This progress is further accelerated by faster hardware with enhanced GPUs and specialized AI chips, making AI more effective at real-time video analysis and high-accuracy threat detection.

Integration of AI with IoT devices and sensors

As security cameras and sensors become more powerful, more data processing can happen within the devices. By embedding machine learning capabilities into IoT devices, AI-powered security systems can autonomously deliver real-time insights and actionable intelligence to security operators. Edge-based processing enables rapid decision-making and reduces latency since data does not need to be sent to a central server for analysis. Additionally, edge processing improves bandwidth efficiency by transmitting only relevant metadata and alerts to central systems.

Rise of predictive analytics in security operations

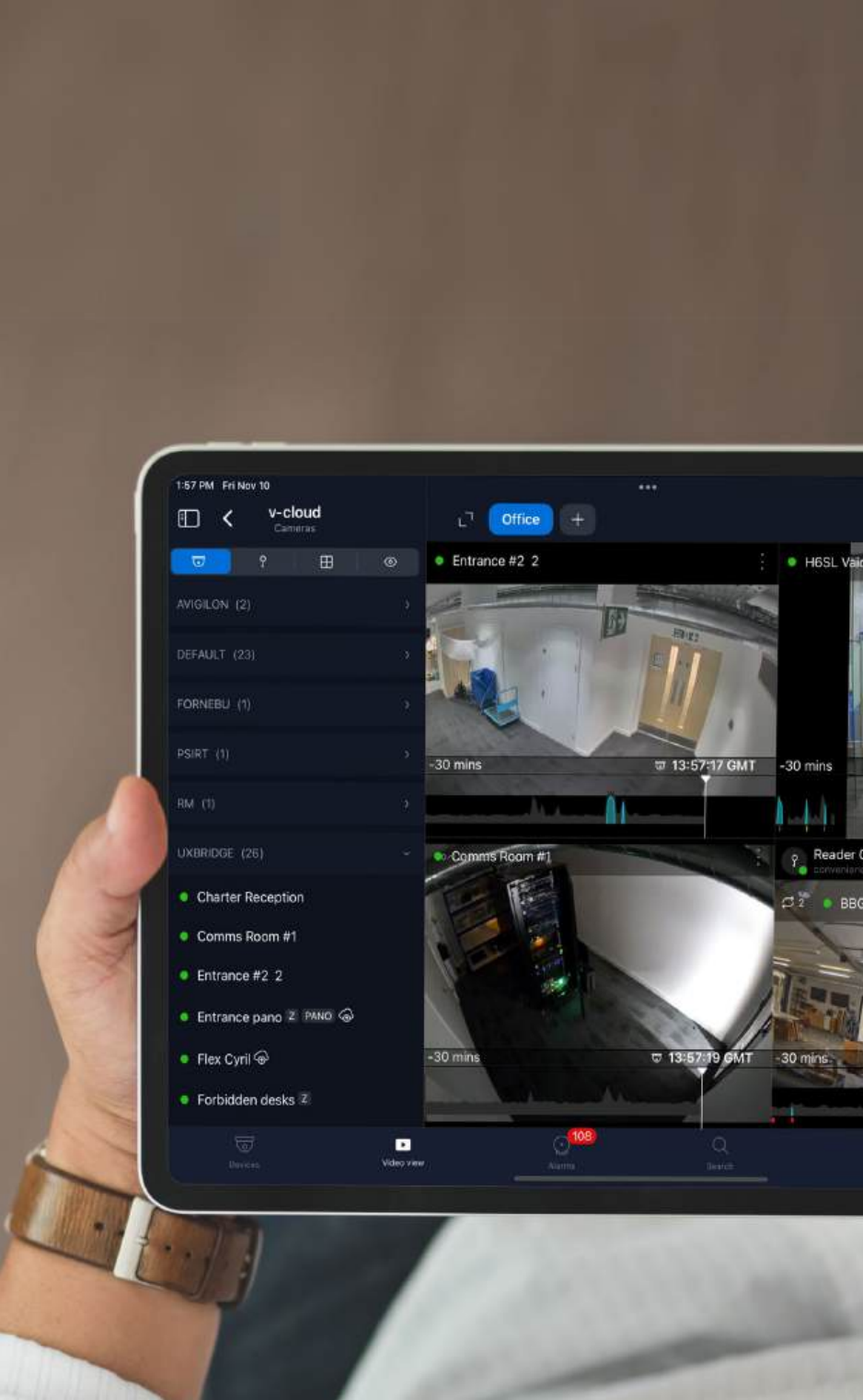
Predictive analytics are a powerful feature of AI-powered security systems that identify threats in real time. These sophisticated algorithms analyze historical and real-time data to identify patterns indicative of security threats. Using anomaly detection, AI can flag irregular behavior or events without being explicitly programmed to look for them. This capability is crucial for anticipating and detecting dynamic threats that evolve over time.



Pushing processing capability to the edge creates a direct, one-to-one relationship between the sensors and their processing power. This means that with each new sensor you add, you're also adding the intelligence.

– Kaveh Malakuti, Senior Director of Product Management, Motorola Solutions





Shift to the cloud

The increasing adoption of cloud-based security systems enables security teams to manage infrastructure across multiple locations through a single interface, regardless of where the physical offices are. Scalability is another key benefit of cloud security systems, allowing organizations to access vast computing power exactly when needed. By hosting security systems in the cloud, organizations benefit from enhanced flexibility, allowing them to deploy AI capabilities more quickly and adapt to evolving security needs.

Convergence of security and operational technology

The integration of AI-powered security technologies with operational technology is changing facility management, particularly in smart buildings. AI enables real-time, automated adjustments that enhance both security and operational efficiency. For example, AI can analyze video footage to adjust lighting and environmental controls, resulting in cost savings and a reduced carbon footprint. Additionally, AI's ability to learn and predict operational routines allows for automated adjustments to security protocols, like managing access based on peak times or employee schedules to minimize bottlenecks and improve visitor experience.

“The cloud offers enterprises—both large and small—the flexibility to be part of an ecosystem that leverages the best technologies available without the need for the costly hardware updates.

— Alex Kazerani, Senior Vice President of Cloud Video Security & Access Control, Motorola Solutions



AI use cases in security technology

Security technology with deep learning capabilities is becoming increasingly common. This section explores how different applications of AI in security technology support human-led decision-making, allowing for quicker and more effective response.

Video security

AI technology helps increase situational awareness and enhance threat detection capabilities. Unlike traditional video security systems, which rely on human operators to monitor video feeds continuously, AI-powered systems automatically analyze video, detecting unusual activities and providing real-time alerts to operators.

AI video analytics can recognize behaviors and patterns that indicate suspicious activities, such as loitering in restricted areas, aggressive behavior or abandoned objects. These insights provide a deeper understanding of the scene, allowing security teams to focus on genuine threats and respond promptly. As AI learns and adapts, its accuracy and effectiveness improve, further supporting security operators' decision-making.

Gun detection technology is a key use case demonstrating the power of AI in video security. AI algorithms can scan video feeds for objects resembling firearms and immediately alert security operators. This capability is particularly valuable in environments such as schools, public venues and workplaces, where rapid detection is critical for the safety of many people.

“Traditionally, physical security has been reactive—investigating incidents like which car hit which car in the parking lot. But with AI, you can leverage feeds from multiple video cameras and AI-driven analytics to notify you of anomalies like a fall, a detected gun, a car accident or unauthorized access. This capability is incredibly valuable, allowing you to respond to alerts that truly matter and create safer environments.

– Alex Kazerani, Senior Vice President of Cloud Video Security & Access Control, Motorola Solutions



Access control

AI transforms access control systems by incorporating advanced features like appearance-based authentication. Instead of relying solely on traditional credentials like key cards or passwords, AI-based systems use biometric data for identity verification. This approach not only strengthens security but also simplifies the access process for users.

Traditional access controls rely on static permissions, which lack the adaptability and scalability necessary for modern hybrid workplaces. AI-driven adaptive access protocols improve the efficiency of security operations by enabling a more responsive and adaptable approach. These systems continuously observe interactions with access points and analyze them in the context of time, location and the user's role. If abnormal behavior is detected, the system alerts security teams, providing the necessary context to support an informed response.

Additionally, AI-powered access control systems can automate response to security incidents. For example, if an individual attempts to access a sensitive area outside of normal hours, the system may trigger additional authentication measures or initiate a lockdown until the threat is verified.

“With video security, we see what’s happening. With access control, we decide who has access to different parts of the building, when and why. Together, they provide a comprehensive view—who came in, who they were with, what they were carrying and who left. AI adds even more value by filtering out the noise and helping detect true incidents, so security teams can focus on the critical alerts that matter most.

– Alex Kazerani, Senior Vice President of Cloud Video Security & Access Control, Motorola Solutions

Site protection

Traditional security systems rely on predefined rules and patterns to identify threats, often resulting in false alarms or missed incidents. In contrast, AI-powered site protection systems leverage insights from audio and AI video analytics to validate alerts and inform faster and more precise response.

Using advanced rule engines, these systems analyze data continuously to differentiate between routine movements and suspicious behaviors. By providing real-time validation of alerts and reducing false alarms, these analytics help security teams prioritize and respond to incidents more efficiently, ensuring a swift resolution to potential threats.

License plate recognition (LPR)

LPR systems are another example of how AI transforms security operations. Using AI and machine learning algorithms, LPR systems capture high-quality footage of moving vehicles and convert these images into readable text, even in challenging conditions. This data is stored and managed by users, enabling your security team to configure custom data-sharing settings to facilitate collaboration with other business partners and law enforcement agencies.

Integrating LPR with existing security infrastructure enhances situational awareness and improves investigative efficiency by providing real-time alerts for vehicles of interest. Within LPR systems, security teams can create and manage watchlists, receive rules-based alerts and conduct rapid post-event investigations.

Additionally, LPR analytics can provide valuable insights into vehicle patterns, helping optimize operations. For example, AI can analyze vehicle flow and parking usage, offering data that improves traffic management, particularly in large commercial spaces and residential areas.





An evolution toward proactive security systems

Security technology allows organizations to increase awareness of their environments and maintain a safer environment for employees, students and visitors. Powered by technological advances, commercial security technology evolved from analog systems that required manual oversight to sophisticated, AI-driven solutions that enable real-time, proactive security management.

The limitations of traditional security systems

In the past, security systems were reactive and often operated in isolated silos, requiring significant human intervention. Imagine a security control room where a security operator observes multiple security camera feeds. Studies show that this way of looking for threats is highly ineffective – after just 20 minutes, an operator watching a video scene will [miss up to 95% of all activity](#).

When an initial event is overlooked, investigations typically begin only after someone notices something out of place – a door left ajar or an object in an unusual location. This means that investigation often occurs hours or even days after the incident, delaying response and limiting your ability to identify and address the root cause of the issue.

As security technology advanced, rules-based analytics allowed security teams to detect specific events or objects by analyzing changes in pixel values over time. However, for a long time, this detection was limited to two classes of objects – humans and vehicles – which led to frequent false alarms from mundane triggers like animals or wind. Additionally, these systems were confined to predetermined rules, making them less effective in adapting to dynamic scenarios and detecting evolving threats.

“A person monitoring multiple screens could easily miss an incident if their attention is not focused on the right thing. AI-driven security technology is on the journey to offload the constant attention to the machine and allow it to alert the operator only when a threat is detected.

– Kaveh Malakuti, Senior Director of Product Management, Motorola Solutions



The power of AI in modern security systems

Today, the landscape of security technology is rapidly evolving towards a more proactive approach. AI-driven analytics leverage machine learning to analyze data in real-time and deliver more accurate and context-aware alerts. By continuously learning from past data, they improve over time, distinguishing between actionable and non-actionable events. As a result of refined accuracy and reliability, modern solutions allow security teams to focus on real incidents rather than monitoring of video feeds and verifying false alarms.

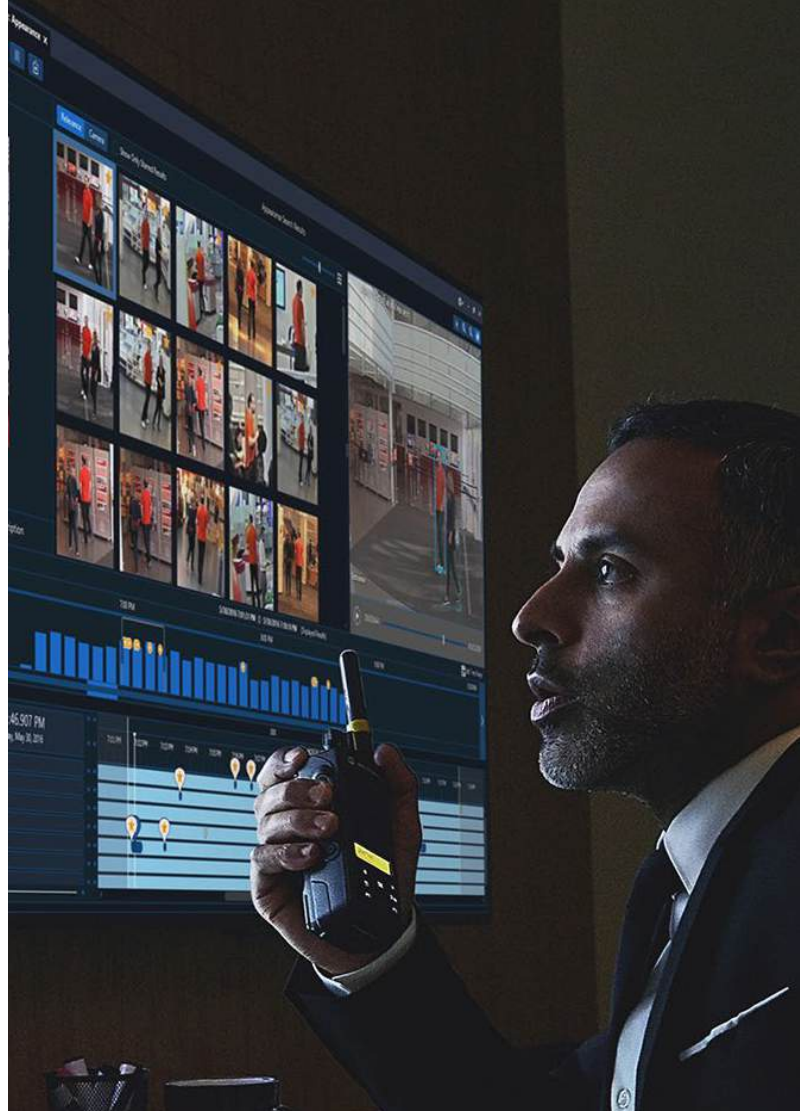
For example, AI-driven video security can identify unusual behaviors, such as loitering in restricted areas or attempts at unauthorized access, and instantly notify security operators for a rapid response. At the same time, adaptive access protocols can dynamically adjust permissions based on real-time data, revoking access rights to secure the area.

The future of security: personalized and contextualized protection

Looking ahead, security systems will use historical and real-time data to generate more precise and context-specific alerts, allowing teams to detect and respond to threats with more efficiency. In complex environments where operators have different roles, AI-powered systems will further accelerate response speed by delivering personalized alerts to the right people at the right time.

This shift toward proactive and focused threat detection marks a significant improvement over the disconnected, reactive systems of the past. By leveraging AI and integrating security technologies, you can create a safer, more efficient environment equipped to anticipate and withstand evolving threats.

However, AI should not be treated as a replacement for human intelligence. Human oversight remains crucial to ensure AI systems are used responsibly and effectively. While AI excels at identifying patterns and generating alerts, human operators provide the necessary context and judgment to validate these findings and take appropriate action.



“We’re moving away from a binary way of detecting objects and relying on a human to judgement determine if it’s a genuine threat. Now we’re augmenting object detection with facial recognition and appearance search, so the system can provide more context and offload some of the decision-making burden from human operators. At the core of it, we’re automating the mundane security tasks to free up human attention for the critical situations.

– Kaveh Malakuti, Senior Director of Product Management, Motorola Solutions





Considerations for implementing AI in physical security

Artificial intelligence is a powerful yet complex technology. Applied carelessly, it can generate unintended results, amplify undesirable outcomes and put your organization at risk. To ensure successful AI implementation and maximize its effectiveness, it's crucial to address key factors such as data privacy, security, integration challenges and ethical implications. Here's a closer look at these key considerations for implementing AI in physical security.

→ Data privacy and security

As IoT devices are increasingly integrated into security operations, they also become prime targets for cybercriminals seeking to exploit vulnerabilities and access sensitive data. Additionally, since AI systems collect and store vast amounts of data, it's important to consider your compliance requirements. For instance, using features like facial recognition may subject you to scrutiny under data protection regulations such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA).

To mitigate cyber risks, remain compliant and maintain stakeholder trust, it's critical to implement robust data protection measures, conduct regular audits and establish transparent data handling practices. Your AI security system software should be regularly updated and patched to reduce the risk of vulnerability exploitation.



→ Integration challenges

To effectively operationalize AI security systems, you need to align your goals against available resources and existing infrastructure. For example, AI-driven analytics need high-quality images to be effective, which may require you to upgrade your cameras to include advanced features like wide dynamic range, high frame rates and efficient streaming codecs.

If your organization has a large number of existing cameras, you will need to decide whether to upgrade them for edge processing capabilities or add appliances to enhance intelligence in your security system. You will also need to assess the capacity of these appliances and determine how many cameras they can support.

Training and upskilling your security operators is another critical challenge. AI-driven systems introduce new tools and workflows that require a different set of skills from your security team. Continuous training programs and upskilling initiatives are essential to empower your team to leverage AI to its full potential.

→ Ethical and social implications

As technology advances, no singular framework or regulation has been set as a standard for responsible AI implementation. This leaves each organization responsible for setting its own guidelines for AI usage, leading to a wide range of applications and opening opportunities for potential misuse. Organizations looking to implement AI in a responsible way need to consider setting strict privacy safeguards and communicating transparently about how AI systems are used to address privacy concerns and maintain public trust.

Ensuring fairness and accountability in AI algorithms is equally important. AI systems, trained on large amounts of data, can inadvertently reflect existing biases, making human validation of AI responses a critical step in technology implementation. To minimize

bias, it's also essential to conduct rigorous testing and use diverse, high-quality training data when building AI models.

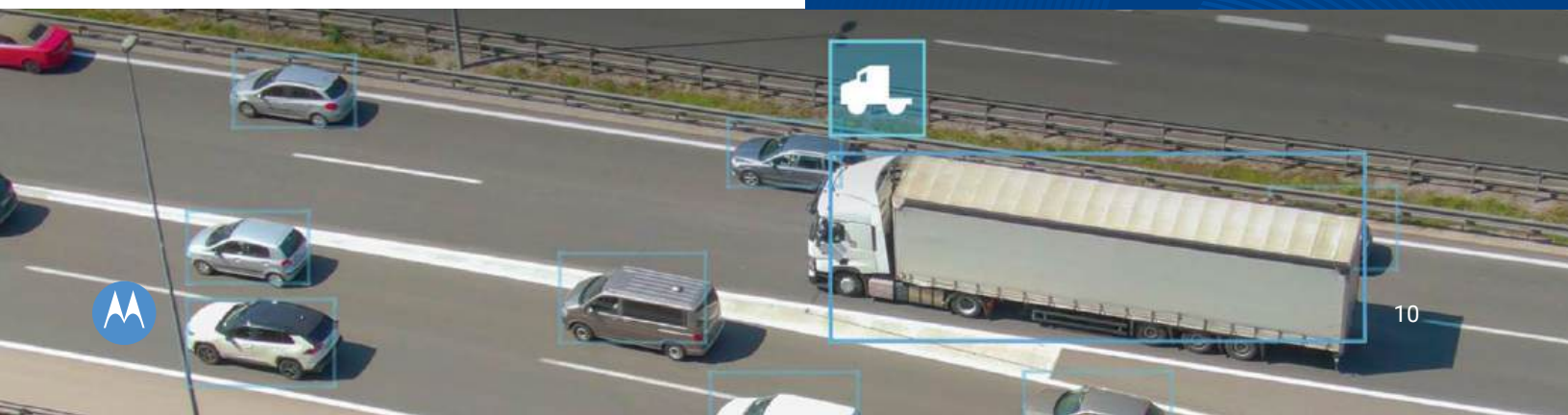
→ Avoiding overreliance on AI

While AI can generate alerts based on data patterns and anomalies, human intelligence is still required for verifying alerts and making nuanced decisions that AI might not be equipped to handle. For example, an AI system might flag an unusual access alert when an employee enters the office at an unusual hour. However, a human operator familiar with the organization can verify that the employee poses no threat and was simply staying late to help with an event.

Organizations looking to adopt AI in their operations should consider implementing a responsible AI policy to guide the ethical and effective deployment of new technologies. This policy should outline the appropriate use of AI, its limitations and the importance of human oversight. Establishing clear protocols for the use and management of AI systems ensures their effective use while mitigating risks associated with overreliance and misuse.

“It's important to consider how AI-driven solutions will work end-to-end and how the outcomes will be delivered at scale. Consider who benefits from the alerts and what it takes to make them actionable. Will you need to manually create rules to identify objects of interest? That is a burden that no one can take on today.

– Kaveh Malakuti, Senior Director of Product Management, Motorola Solutions



Avigilon solutions that are moving the needle

Avigilon and Motorola Solutions' ecosystem of security solutions integrates AI technologies to accelerate your workflow with real-time threat detection and response capabilities. Our AI solutions are purpose-built with a "human-in-the-loop" approach to assist and augment your security team's capabilities. Below are some examples of the latest AI-driven Avigilon technologies designed to proactively address modern security needs.



AI-enabled IP cameras

Avigilon offers a wide range of IP cameras with different form factors, lenses, resolutions and storage to meet nearly every deployment need. All cameras feature AI-powered analytics tools that quickly alert you to anomalies and potential threats. Designed to provide crystal-clear footage, these cameras help you see important details, even in challenging conditions. Multiple styles of camera hardware can be installed and linked to provide comprehensive coverage of multiple sites.

[View Avigilon security cameras](#)



Avigilon Unity Video

Avigilon Unity Video is a robust AI-powered video management software (VMS) designed to enhance real-time insights and situational awareness. This on-premise solution seamlessly integrates with access control, decision management and cloud services to provide a comprehensive platform for managing security operations across multiple sites.

With Unity Video, security teams can detect critical events, locate persons and vehicles of interest, and identify suspicious activity from a single platform supported by real-time AI technology, AdaptAI. The Focus of Attention interface uses AI to prioritize and display the most relevant footage, ensuring that security operators are immediately aware of situations requiring attention. Appearance Search allows users to locate a person or vehicle across multiple sites by entering physical descriptors, making it easier to track movements and gather information quickly. License Plate Recognition automatically reads and links license plate data to live and recorded video, providing instant alerts when a vehicle of interest is detected.

[Explore Avigilon Unity Video](#)





Avigilon Alta Video

Avigilon Alta Video is a powerful AI-driven VMS that enhances security by providing real-time visibility and actionable intelligence across your entire organization. As part of the Avigilon Alta cloud security suite, Alta Video integrates seamlessly with your existing hardware and third-party devices, offering a flexible and scalable solution for modern security challenges.

The platform's intelligent algorithms and self-learning capabilities continuously analyze video feeds to identify abnormal behavior in real time and proactively identify threats so you can take action before they escalate. Avigilon Alta analytics leverage both VMS and edge processing to enable faster response times and allow for more cost-effective processing. Alta Video also offers smart, intuitive search tools to accelerate investigations and empower your security operators to find objects of interest quickly.

In addition to detecting threats, Alta Video leverages AI-driven tools like audio analytics and occupancy monitoring to enhance operational awareness. You can use the data insights from video analytics and sensors to optimize business processes and improve the customer experience.

[See Avigilon Alta Video](#)



Avigilon Alta Protect

Avigilon Alta Protect is an advanced, AI-powered site protection system designed to provide you with a proactive approach to security. By integrating AI-driven video and audio analytics with sensor data, Alta Protect enables swift detection and response to suspicious activities such as loitering, unauthorized access and vandalism.

Avigilon Alta Protect uses AI video analytics to validate alerts and minimize false positives. The system's powerful rules engine allows for the creation of custom alerts based on zones, schedules and specific detection parameters. By leveraging existing AI-powered cameras and integrating with additional sensors, Alta Protect reduces the need for extensive physical infrastructure while enhancing overall security capabilities.

[Explore Avigilon Alta Protect](#)

“At Motorola Solutions, we are dedicated to compliance and security. We take pride in our SOC2 and ISO compliance, as well as continuous pen testing on our platform. We also manage GDPR and CCPA obligations to support companies with their privacy needs. The security we provide is unmatched—a fact our multinational enterprise clients greatly appreciate.

– Alex Kazerani, Senior Vice President of Cloud Video Security & Access Control, Motorola Solutions





Case studies

Find out how leading organizations utilized Avigilon's AI-driven physical security solutions to address their most pressing safety and security challenges.

Superdry secures global retail operations with Avigilon Alta

Superdry, a global retailer with over 220 stores, faced challenges in securing stores with high foot traffic and preventing theft. To address these issues, the company turned to Avigilon Alta for a comprehensive video security solution. By integrating Avigilon Alta's advanced AI analytics and high-resolution cameras, Superdry enhanced situational awareness and improved operational efficiency.

The AI-driven features, such as video search and heat mapping, allowed the security team to detect suspicious activity in real-time, reducing losses and increasing store safety. Additionally, the cloud-based system also facilitated seamless collaboration between remote security teams and in-store staff, ensuring Superdry's expansive operations remain secure as the company grows.

[Read case study](#)

“

We chose the Avigilon Alta cloud-based solution because the technology is open, flexible and scalable. We could integrate our existing video security cameras to the new system and can easily add more cameras as we expand, which made Avigilon the right choice for us today and in the future.

– Richard Smith, Profit Protection Manager at Superdry





With crystal-clear video and a VMS that combines AI intelligence with cloud capabilities, we are better placed to effectively handle our security operations across our entire facility.

– Richard Lundgren, Technical Manager at Deep Dive Dubai



Deep Dive Dubai enhances safety with Avigilon Unity

Deep Dive Dubai, home to the world's deepest diving pool, sought to build a robust security system and help visitors enjoy a unique diving experience. They implemented Avigilon Unity, integrating 56 H5A Box cameras and the Unity VMS. The high-resolution cameras, equipped with AI-powered analytics, allowed the security team to improve the situational awareness of the pool, even in low-light conditions. This advanced technology enabled the team to detect and respond to potential threats swiftly, helping ensure the safety of divers and the security of the facility.

The Unity Video VMS further optimized security operations by providing real-time insights and remote access through Unity Cloud Services. This setup enabled more efficient incident management, reducing response times to critical events. The improved video quality and analytics also supported additional operations, such as hosting commercial events, demonstrating the system's versatility and effectiveness in a demanding environment.

[Read case study](#)

Smarter, AI-powered security at Guayaquil Airport

Guayaquil's José Joaquín de Olmedo International Airport, managed by TAGSA, sought to modernize its security system to better protect passengers, staff and air operations. By implementing Avigilon Unity Video, the airport enhanced its security posture with AI-driven video analytics.

The integration of Avigilon's appearance-based search and facial recognition technology enabled security teams to identify individuals flagged in the airport's database, helping prevent incidents before they escalate. Additionally, deploying high-resolution cameras and thermal imaging has improved surveillance in critical areas, ensuring comprehensive coverage across the airport's extensive facilities.

[Read case study](#)



Conclusion

As security threats become more complex, the need to build a proactive security posture becomes critical for many organizations. The advancements in AI-driven security solutions brought on by sophisticated deep learning algorithms and edge computing enhance the reliability and accuracy of facial recognition, object recognition and behavior analysis. These advancements allow you to detect suspicious activity and respond to threats before an incident takes place.

However, successful implementation requires careful consideration of data privacy, integration challenges and ethical implications. It is also important to treat AI as a way to support human decision-making rather than replacing it. In fact, organizations that benefit the most from these new technologies use AI-driven technologies to complement human intelligence by enabling security teams to work more efficiently



To explore how Avigilon's AI-powered solutions can transform your security operations, speak with one of our experts today.

Visit www.avigilon.com to learn more



AVIGILON™

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. motorolasolutions.com

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. ©2024 Motorola Solutions, Inc. All rights reserved. 09-2024 [JMS02]