



Guide

Unlocking security: a guide to the latest technology

New industry trends for 2026

Stay informed on the latest security trends for 2026 and read how you can enhance the safety of your organization while simplifying processes with the cloud, artificial intelligence, unified security and more.



Industry trends for 2026

Physical security has always been top of mind for those overseeing office operations and other commercial buildings. From preventing crime to ensuring a better overall experience, new security technologies make it easier than ever to protect both residential and commercial properties effectively.

However, it has never been more important to ensure your security systems are cybersecure. Cybercrime continues to be a major global issue and it's evolving quickly. Attackers are now using artificial intelligence (AI) to craft convincing scams and design malware that constantly changes to avoid detection. These AI-powered attacks have become a primary way that organizations are breached. This is why it's now essential to unify your physical security with your digital security.

According to the Cybersecurity and Infrastructure Security Agency, cyberattacks cost commercial businesses in the U.S. \$394,000 to \$19.9 million per incident. This is compounded by physical security failures, with the World Security Report finding that over \$1 trillion in revenue was lost by companies as a result of physical security incidents.

With the increasing usage of connected devices, IoT and AI technologies in security, safeguarding data both in motion and at rest is a crucial objective that will influence the development of new trends in security technology and cybersecurity.

Luckily, there are many ways to mitigate risk with new security technologies. Implementing a combination of physical security, cybersecurity and IT security technologies can provide a much-needed layer of protection.

While there is no 'one-size-fits-all' approach to security and every company has different needs, new high-tech security trends of 2026 can help businesses find new security technologies to protect their assets and uncover solutions to their most pressing challenges.



What is security technology?

Before looking at the emerging security technology trends of 2026, it's important to understand how this sector differs from others.

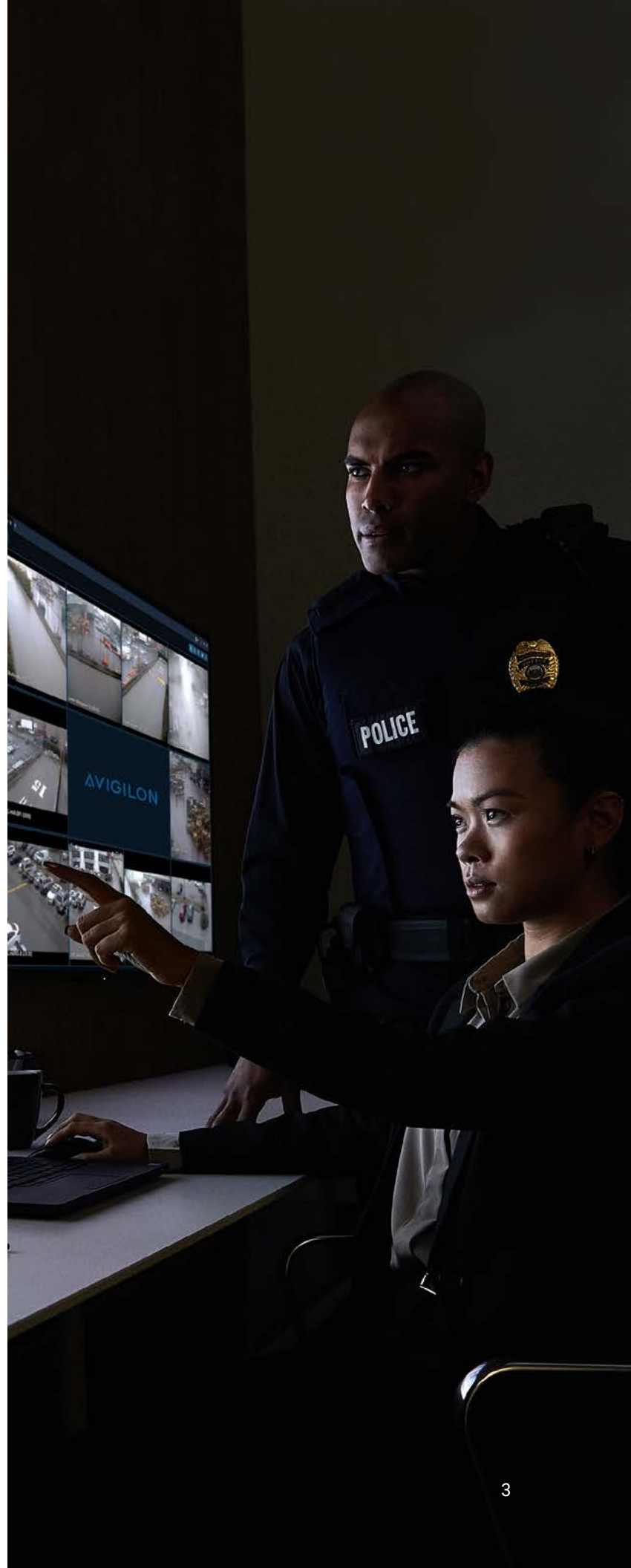
Security technology refers to the components and policies used to protect data, property and assets. Security technology helps mitigate risk by preventing unauthorized access, identifying potential incidents, allowing fast responses, deterring criminal behavior and capturing crucial evidence.

Advanced security technologies can be used to secure physical assets and electronic data, both on-site and remotely.

In order to protect yourself and your business from security breaches, it is imperative to understand how the security in technology components of your systems can strengthen or weaken your other strategies.

Physical security technology examples include:

- Access control systems and intrusion detection
- Electronic and wireless locks
- Credentials including key cards, key fobs and mobile devices
- Environmental and motion sensors
- Alarm and emergency systems





The importance of cybersecurity

As the digital landscape continues to evolve, businesses must remain up to date with the current cybersecurity and information trends of 2026.

Cybersecurity technology helps defend business networks, data and devices from malicious attacks and fraudulent activity. Common cybersecurity technology examples include:

- Encryption
- Ransomware detection
- Spyware monitoring
- IT security analytics

While traditional antivirus and firewall software remain foundational, the new security technology trends for 2026 point to predictive and adaptive solutions, leveraging AI and machine learning to anticipate threats before they breach the perimeter.



The importance of information security technology

Data security technology and IT security technology are cybersecurity practices and systems that protect information and networks from unauthorized access or disruption. This sector relies on both physical and cybersecurity measures.

Effective information security technologies should detect and prevent unauthorized access to security data, protect the integrity of the data and ensure compliance with regulatory requirements. Generally, the goal is to ensure that only authorized users have access to specific data.

Examples of information security technologies and policies include:

- Network segmentation
- Firewalls
- Anti-malware software
- Data loss prevention software
- Password protection and authentication

Ultimately, information security technologies provide a multi-faceted approach that requires the use of specialized technologies and well-defined policies.



What factors are influencing security technology trends in 2026?

When it comes to recognizing new trends in security technology, certain factors will always drive what's popular. Most often, security technology trends are driven by the latest vulnerabilities.

That being said, the security technology trends of 2026 also reflect new ways organizations conduct their business. Economic and social trends often change people's expectations of how and when they work, which can drive exponential advancements in security technology.

Below are the top five factors influencing new security technology trends for 2026:

- Increased adoption of cloud-native security technologies
- Growth in the application of AI and machine learning
- Efficiency gains achieved from unifying security systems
- Normalization of hybrid and remote working creates dispersed teams
- Continued shift to information security technologies with zero-trust network access

To find out how businesses are balancing security and technology, let's examine what technology ranks highest on the industry's security trends for 2026.



Top security technology trends of 2026

You may be familiar with some of the latest physical security technologies, as they tend to play a major role in day-to-day life. [IP security cameras](#) and alarm systems are some of the most common security technology examples, but additional tech trends are appearing within modern physical security systems, such as:

Cloud-native security solutions

The cloud continues to revolutionize how businesses store and share information. As one of the leading security trends of 2026, true cloud-native platforms, as opposed to simply cloud-hosted legacy systems, are facilitating streamlined multi-site management, integrated security technology solutions and enabling fully remote security operations.

As a result, businesses and security teams can access, manage and control their security operations from anywhere at any time. This is often paired with edge computing, where AI processing happens on the device itself, to reduce latency and data transmission, reserving the cloud for centralized management and complex analytics.

Security managed through the cloud, such as [cloud-based video security systems](#), also extends to maintenance and system availability. Businesses receive real-time notifications to their mobile devices should a security camera malfunction or a server go down.

While cloud security has helped businesses accommodate flexible work models, it also comes with risks. As businesses rely more heavily on the cloud, they must strengthen their security measures to protect against data loss and hacking threats. Implementing security solutions such as intrusion detection systems, [door access control systems](#) and advanced data encryption can ensure a business's information is secure and well-protected.





Embracing AI and machine learning

AI and machine learning capabilities are crucial in ensuring the global security of business operations and customer data. AI technologies can detect network traffic and data anomalies and monitor user behaviors for any suspicious activity from both a cyber and physical security level.

The industry has already seen massive leaps in the accuracy and reliability of AI-powered video cameras. This intelligent technology makes passively watching live video obsolete. Security systems can accurately detect and classify people, vehicles and objects, as well as pinpoint their locations and enable faster forensic searches. Latest AI technology shows it is now possible to detect the presence of weapons. From a business operations point of view, AI can provide key insights that can help drive revenue and cut inefficiencies through heat maps, people-counting and activity logs.

The real benefit of this 2026 security industry trend comes from integrating AI-powered devices and systems for centralized management of the entire enterprise within a single platform.

Machine learning also continues to be an important component of new information security technology trends of 2026 and can be found in many [license plate recognition systems](#) and video management solutions. By continuously monitoring the network for suspicious activity and providing an automated response, security teams can stay informed in real-time.

With the rise of generative AI, businesses must be aware of the cybersecurity and privacy risks. Camera networks are playgrounds for malicious hackers, and steps must be taken to protect the infrastructure, including encryption and installing the latest software updates.

Unifying security systems

In recent years, companies have started integrating various security systems with new [access control trends](#) to enhance safety. The obvious unification is integrating video security with access control to synchronize footage with access events.

However, true unification goes beyond simply linking video with access control. The real power comes from connecting your entire ecosystem of technologies. For example, integrating two-way radios with your video security and access control platform can automate alerts and dramatically speed up response times.

By breaking down these technology siloes and bringing them together on a single platform, security teams can simplify management and automate workflows. This trend is also visible in hardware, where all-in-one [video door intercom systems](#) now combine a camera, access reader and intercom into a single device.

The key to achieving this is choosing security solutions built on an open platform. This design ensures that new technology can seamlessly integrate with your existing systems. This means you don't need to rip and replace your current hardware, saving you significant time and money.





Future-proofing through scalable solutions

An additional security and cybersecurity technology trend of 2026 is future-proofing video security. Cost control is an integral part of running a successful business. Therefore, future-proofing on-premise and cloud-based video security technologies is crucial to ensuring security investments continue to pay off in years to come.

Scalable and flexible solutions allow users to select license packages to suit their needs, whether it's a small-to-medium business that requires a small number of security cameras or a global enterprise that requires thousands. Security solutions can scale up with the growth of the business and allow security teams to easily adjust their systems without breaking the bank.

Future-proofing your security systems also ensures they stay protected from future cyberattacks. As new threats develop, your systems must be updated. A key 2026 consideration is crypto-agility. Think of this as ensuring your system's digital encryption can be easily swapped. This is crucial, as new threats, such as powerful quantum computers, are on the horizon and could one day break today's encryption.

Crypto-agility means that when that day comes, you can simply patch your system with a new, stronger encryption instead of having to replace everything.

Privacy and data protection

As security technology evolves, privacy and compliance take on greater importance, particularly with video. As seen with the U.S. government [banning](#) Chinese security cameras and equipment due to national security concerns, organizations are prioritizing security solutions that meet compliance and privacy requirements, such as NDAA section 889 compliance.

It's never been more important to be aware of security's legal and ethical consequences. From the placement of a camera to the management of data and facial recognition, regulations worldwide are becoming more stringent. Businesses should account for this when procuring a new security solution or upgrading their legacy system.

Thankfully, there are security providers that comply with global regulations and are built with Privacy by Design. These offer features like dynamic video anonymization, blurring faces until an incident is flagged, and granular, role-based access to data to ensure compliance with GDPR and new state-level data laws while protecting people and assets.





User behavior analytics

User and entity behavior analytics (UEBA) is a trend gaining significant attention in the security industry, given its ability to detect even the most sophisticated threats. Using machine learning algorithms, UEBA can detect any unusual behavior from users, applications and networks, and alert teams to potential dangers in real time.

By understanding how users interact with systems, businesses can quickly identify and remediate any threats before they cause damage. UEBA systems are an advancement from User Behavior Analytics (UBA) systems that only analyzed user behavior. They are an important trend in the 2026 cybersecurity industry, as they offer more complex reporting and greater capacity to spot anomalous behavior.

Digital identity as the new perimeter

In 2026, the traditional security perimeter, such as office walls and firewalls, has been dissolved by hybrid work. The new perimeter is now the individual's digital identity.

This trend moves beyond separate physical key cards and digital passwords, introducing Unified Identity. This approach uses a single, verified credential, often on a mobile device, to grant access to everything from laptops and cloud servers to physical doors.

The convergence is critical: if a user's digital account is compromised, the system can automatically and instantly revoke their physical access to the building, closing a major security gap.

Additionally, the trend is driving continuous, frictionless authentication. Instead of verifying a user once at login, systems now use behavioral biometrics, like typing patterns or gait analysis, integrated with User and Entity Behavior Analytics (UEBA).

This allows the system to passively observe user behavior in the background. If a hacker hijacks an active session,

their behavior won't match the user's profile. The system can detect this anomaly mid-session, lock the account and prevent the breach in real-time.

AI video analytics

Over the past few years, AI has moved from a buzzword to an essential mainstream tool, and its implications for the future of security cannot be ignored.

The security industry is experiencing a surge in demand for artificial intelligence (AI) in cameras and comprehensive physical security systems. While AI cameras are already being used in various applications, new advancements in this technology for security are making AI more valuable for businesses that previously felt they didn't need it. The latest AI security technology for various camera types, including [bullet IP security cameras](#), can accurately recognize abnormal behavior and differentiate between people, vehicles and objects, generating location and movement data, as well as sending automatic alerts to keep teams more informed.

AI security technologies are also being used in smart sensors to help property owners identify vaping incidents in schools, broken glass and gunshots, with sound detection analytics helping determine where the incident is taking place. The real benefit of this 2026 security industry trend comes from integrating AI-powered devices and systems for centralized management of the entire building or enterprise within a single [video management software](#) platform.

Because these future-forward devices leverage incredible amounts of data to analyze complex and changing elements of their environments, the longer they are active, the more accurately they can identify potential security threats. However, all this data in the wrong hands could prove to be a serious problem. That's why another security technology trend in 2026 to watch is how cyber and physical security teams are leveraging AI technology to proactively monitor networks, modernize security auditing, optimize monitoring systems and inform threat prevention strategies.





Smart sensor technology

The role of smart sensors is becoming increasingly pivotal in security. These advanced devices are equipped with the ability to detect environmental changes and security threats, transforming how we approach security in various settings.

Smart sensors like the [HALO Smart Sensor](#) are ideal to combat the rising issue of vape use in schools, but have expanded functionalities beyond vape detection. The sensors also detect environmental changes, such as air quality fluctuations, sound anomalies that could indicate aggression or bullying and chemical presence like cigarette smoke.

The significance of smart sensors and emerging security technologies like advanced [vape detectors](#) lies in their ability to operate in privacy-sensitive areas, such as bathrooms and locker rooms, while traditional security technology solutions are either impractical or intrusive. This capability is crucial, particularly in educational environments where maintaining student privacy is as important as ensuring their safety.

The integration of smart sensors into broader security systems offers an additional layer of protection. By continuously observing changes in the environment, these sensors can provide real-time alerts and enable swift responses to potential threats. This not only enhances overall security, but also helps institutions stay ahead of emerging challenges that will likely shape the future of security tech trends.

Mobile-first technology

Last, but not least, mobile-first technology is predicted to be a key physical security trend for 2026 and will be front of mind for businesses looking to secure their premises. In a world dominated by mobile technology, the demand for apps that enable remote security monitoring is no longer the exception, but the rule.

Businesses with multiple sites or security teams on the move will benefit most from remote monitoring capabilities, as they can access live and recorded video footage across multiple sites from the palm of their hands and easily carry out tasks.

Most mobile systems, such as [mobile credentials](#), are managed in the cloud, giving operators greater flexibility in managing their security. In addition, people find mobile systems easy to operate. Either by tapping a button in an app or by using touchless options, mobile-based security is convenient, fast and reliable.

As mobile adoption continues to increase, future trends in technology will include even more advancements for mobile-based systems, making them even more secure and interoperable with other building systems.





Avigilon systems to strengthen safety and create unified security

Video security

Avigilon's wide range of security cameras offer high-definition video with advanced features to boost safety and security for various environments. The cameras are equipped with AI-powered video and audio analytics that can detect and classify objects like people, vehicles and unusual activities or sounds (e.g., tires screeching, glass breaking) in real time, helping security teams respond more efficiently.

Integrated with Avigilon's Video Management Software (VMS), the system enables proactive security and allows users to quickly search through footage, identify potential threats and prevent incidents before they escalate. These features improve situational awareness and reduce response times while offering actionable insights for more effective security operations across a wide range of industries.

Additionally, the system can seamlessly integrate with other Avigilon and third-party solutions, providing a unified platform for comprehensive security management across facilities.

Access control

Avigilon access control solutions provide a secure and scalable way to manage entry points across facilities and

ensure only authorized personnel can access restricted areas. The system integrates seamlessly with other security tools, including Avigilon's video security to create a comprehensive platform that improves visibility. Real-time viewing and detailed access logs also enable security teams to quickly identify and respond to potential threats.

With flexible deployment options, including cloud-based and on-premise systems, Avigilon access control is designed to adapt to the needs of any organization, improving operational efficiency while safeguarding people, property and assets with ease.

Video Management Software (VMS) with advanced analytics

Avigilon's VMS unifies security by integrating with cameras and access control, enabling proactive security and faster investigations. The system is equipped with powerful, AI-powered analytics to identify potential threats in real time. Key analytics include appearance search, which allows operators to quickly find a person or vehicle of interest across an entire site based on physical descriptors, and unusual activity or anomaly detection, which flags atypical events that might otherwise be missed.

Additional analytics, like a person crawling or unusual crowd detection, can alert teams to unauthorized access





or unsafe gatherings. With facial recognition and watch list capabilities, the VMS can also send alerts for persons of interest that appear on-site. This improves situational awareness and reduces response times.

Generative AI

Avigilon's Generative AI-powered Visual Alerts offer advanced analytic capabilities, moving beyond predefined rules by allowing operators to create alerts using natural language.

Teams can configure detection for specific scenarios by describing the event (e.g., "alert me when there's a liquid spill" or "alert me when a fire exit is blocked"). This approach is designed to reduce complex configuration time sitewide and provides greater flexibility. By removing the constraints of predefined rules, the possibilities for custom detection are virtually limitless, enabling operators to focus on and respond to the specific events that matter most.

Site protection system

Traditional alarm systems typically rely on contact or motion sensors, which often lead to false alarms triggered by harmless movement or weather. They also lack visual verification, leaving security teams without insight into what caused the alert.

Avigilon's site protection solution, Alta Protect, overcomes these challenges by leveraging Alta cameras and analytics to intelligently detect and verify incidents in real time. This process accelerates responses and minimizes false alarms. For sites without dedicated security teams, Alta Protect's 24/7 professional monitoring service provides round-the-clock protection, with trained security experts verifying alarms and dispatching first responders when needed.

Visitor management systems

The Avigilon Alta Visitor Management system streamlines the guest experience without compromising building security. It allows for the pre-registration of guests, who receive a mobile QR code for frictionless check-in upon arrival. The system enhances safety by enabling ID validation, background checks and the printing of custom badges.

Integrated directly with video security and access control, it provides a complete audit trail of visitor activity. Hosts are automatically notified when their guests arrive, creating a professional, secure and efficient process for managing all non-employee traffic across a facility. Security teams can also link cameras to visitor logs to support compliance and incident response.

Mailroom management systems

Avigilon's Alta Mailroom system streamlines package deliveries for buildings using an intuitive mobile app and web dashboard. Staff can simply scan package labels with a smartphone, which automatically logs the delivery and sends an instant notification to the recipient.

This automated workflow provides a complete, searchable audit trail, helping to reduce mailroom clutter, prevent lost packages and ensure recipients are promptly informed. The system also supports pick-up verification and integrates with existing identity providers to keep user directories synchronized. As part of the broader Avigilon ecosystem, it can work alongside access control and video systems to securely manage carrier entry and investigate any delivery incidents.



Smart sensors

Avigilon's versatile smart sensor, Halo Smart Sensor, is designed to detect environmental and air quality changes to strengthen safety in privacy-sensitive areas like restrooms and locker rooms. Equipped with advanced sensors, it can detect vaping, smoke, chemicals and changes in air quality without using cameras, helping to maintain privacy.

The Halo sensor also monitors noise levels, identifying instances of aggression or disturbances. Integrated with Avigilon's video security systems, it provides real-time alerts for quick response to potential threats and helps facilities comply with health and safety standards.



License Plate Recognition (LPR)

The Avigilon License Plate Recognition (LPR) solution offers automated detection and license plate readings to improve security and operational efficiency. With AI-powered technology, the system accurately captures license plate data in various conditions, day or night. Integrated with Avigilon's video security and access control, LPR enables seamless monitoring of BOLO vehicles with watch list capabilities or set-up license plates as an access credential, allowing security teams to oversee, manage and control access to facilities. This solution improves perimeter security to enhance the overall safety of any site.





How organizations globally rely on Avigilon solutions

Read how the Avigilon security suite helps organizations enhance security and keep people and assets safe while providing key operational and business insights.

Olav Thon Group builds a stronger security foundation with Avigilon

The Norwegian commercial real estate, hospitality and retail company Olav Thon Group's rapid expansion across Norway and Europe required a scalable, unified security solution. Their previous security systems were siloed, inefficient and unable to integrate effectively. The Group chose Avigilon to manage security across their shopping centers, parking lots and hotels.

Avigilon's unified platform allows seamless operation without switching between software, helping to save time and money. Security teams can quickly verify incidents in parking lots, while the video management software speeds up post-event analysis by searching hours of footage in seconds. The data also supports better business decisions and boosts customer satisfaction and store revenues.

[Read case study](#)



With Avigilon Alta technology, we no longer need to invest in a separate security system at each shopping center, saving us a substantial amount of money.

Ola Stavnsborg, Group Security Manager at Olav Thon Group





The University of Tennessee safeguards its campus with Avigilon

With over 27,500 students and a 550-acre campus, the University of Tennessee (UT) needed a robust video security solution to ensure safety during events, particularly at its football stadium. UT implemented the Avigilon security system to enable security personnel and law enforcement to observe campus security in real-time.

Avigilon cameras provide clear footage and act as a deterrent to potential troublemakers. Security teams can analyze live and recorded video using the Avigilon video management software for informed incident response. The system is scalable, ensuring its effectiveness as the university expands. On game days, Avigilon supports monitoring of up to 130,000 fans, strengthening safety before, during and after events.

“ The University of Tennessee is committed to keeping its campus safe, and the Avigilon system is an important part of our security procedures and emergency management plan.

Brian Browning, Director of Administrative and Support Services at University of Tennessee

[Read case study](#)



TAGSA airport in Ecuador raises security standards with Avigilon

TAGSA, covering 180 hectares and serving 3.8 million passengers annually, is a key international airport in Ecuador that faces threats from organized crime. To maintain its high service standards, TAGSA invested in the Avigilon security system to enhance safety for passengers, staff and air operations.

The system provides improved coverage with high-resolution cameras for better threat detection, including locating unattended luggage and lost items. It also aids forensic investigations with clear footage. With Avigilon, TAGSA enhances the passenger experience and ensures safer, more efficient travel.

[Read case study](#)

The future of security technology trends

Businesses need to be constantly aware of the evolving risks associated with physical and cybersecurity threats. Mitigating that risk starts with a [comprehensive security convergence plan](#) to create an effective defense against a range of potential security threats.

Leveraging the latest security technology trends can help organizations with a more proactive approach. The future security technology trends of 2026 point to more collaborative, integrated and holistic systems, providing security teams with more data than ever. That's why investing in AI-powered technology is an important trend to follow – with automation, integrations and true cloud-native technologies helping businesses understand behavior patterns, make informed decisions and respond swiftly to incidents.

Such protections may involve significant upfront investments, but keeping up with future technology trends in security can save an organization time and costs in the long run. Additionally, adopting strong security measures can help boost customer confidence.

Related resources

Click the links to directly access marketing material.

- [Different types of CCTV cameras guide](#)
- [Cybersecurity best practices for access control](#)
- [Intrusion alarm system guide](#)
- [Physical intrusion detection systems guide](#)
- [Guide to vape detectors](#)

Get expert help **today**



AVIGILON™

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

© 2025, Avigilon Corporation. All rights reserved. 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. 11-2025 [PC01]