Unlocking security: a guide to the latest technology

New industry trends for 2025

Stay informed on the latest security trends for 2025 and read how you can enhance the safety of your organization while simplifying processes with the cloud, artificial intelligence, unified security and more.

MOTOROLA SOLUTIONS

AVIGILON

Industry trends for 2025

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, as cybercrime continues to be a global issue and a driving force in the security, cybersecurity, and information security trends of 2025.

In fact, a staggering 49% of breaches by external actors involve the use of stolen credentials and 24% of all breaches involve ransomware – the process of maliciously encrypting data and demanding a ransom to reinstate access. According to the Cybersecurity & Infrastructure Security Agency, cyberattacks cost commercial businesses in the U.S. $394,000 to $19.9 million per incident.

With the increasing usage of connected devices, IoT and AI technologies in the field of 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.

Unfortunately, many businesses fail to sufficiently protect themselves from physical security threats, as well. The World Security Report found that over $1 trillion in revenue was lost by companies as a result of physical security incidents and one in four publicly-listed companies reported a drop in their value following an incident.

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 from damaging breaches and threats.

While there is no ‘one-size-fits-all’ approach to security and every company has different needs, new high-tech security trends of 2025 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 2025, 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 in the event that a breach occurs.

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 2025 to adequately safeguard their security data and operations. The future of cybersecurity is full of potential, but organizations must take proactive steps to ensure their data is safe and secure.

Cybersecurity technology helps defend business networks, data and devices from malicious attacks and fraudulent activity. Network, application and information technologies all play an important role in how effective a cybersecurity strategy is. Common cybersecurity technology examples include:

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

In the past, cybersecurity technology trends were limited to new versions of antivirus and firewall software. However, the new security technology trends for 2025 point to more robust solutions equipped with AI and machine learning.

The importance of information security technology

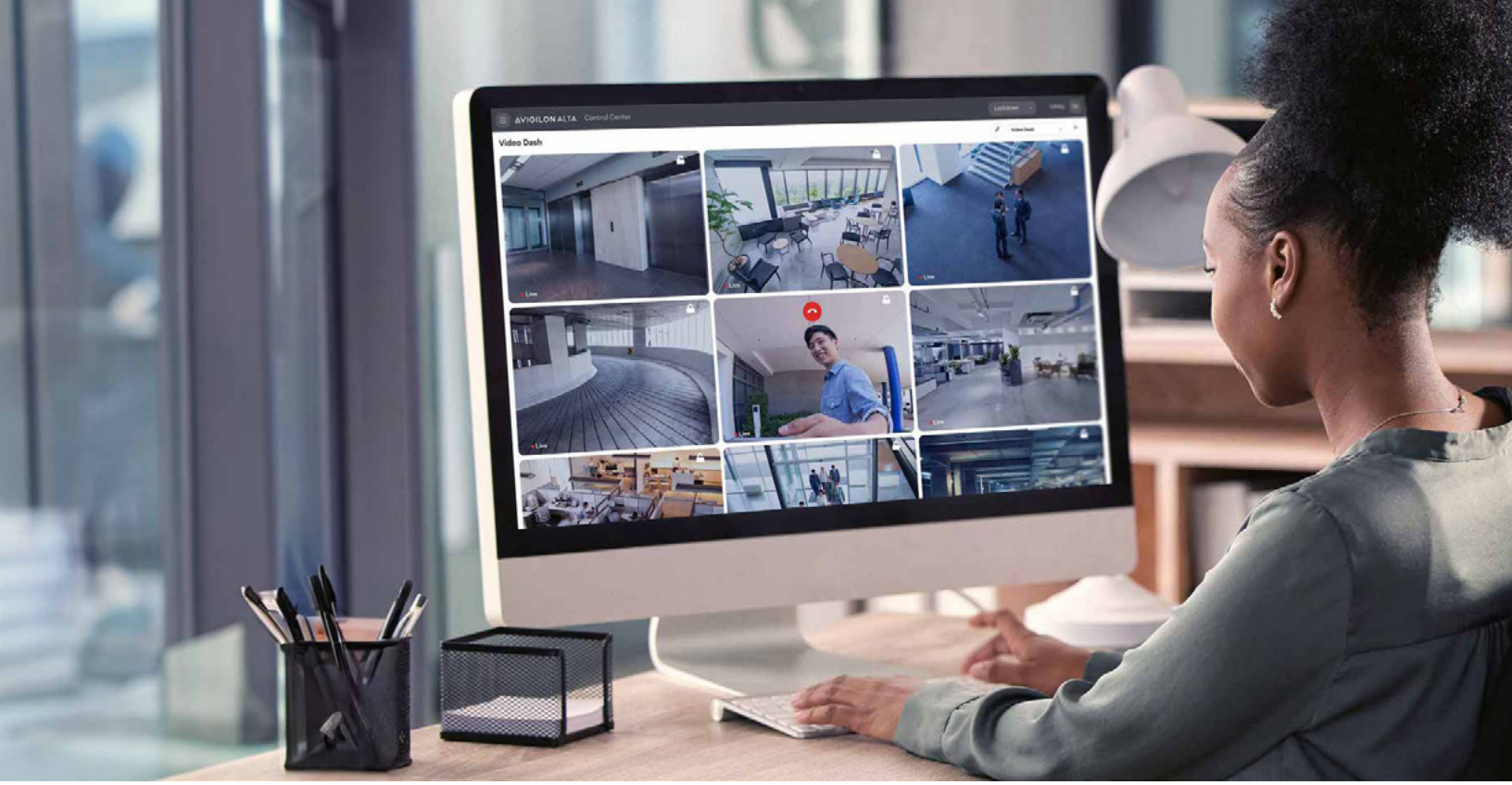
Data security technology and IT security technology are cybersecurity practices and systems that protect information and networks from unauthorized access or disruption. This sector relies on both physical and cybersecurity measures. It is composed of a wide range of system control and protective measures used to safeguard critical information and infrastructure.

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. In addition, they should protect against data alteration or destruction. Generally speaking, the goal is to ensure that only authorized users have access to specific data and that it is protected from corruption.

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 2025?

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. No business wants to fall victim to a known hack or fail to stop a theft due to outdated security tech.

That being said, the security technology trends of 2025 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 2025:

- Increased adoption of cloud-based 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 2025.

Top security technology trends of 2025

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. Many office spaces and commercial buildings feature a number of physical security technologies. IP security cameras and alarm systems are some of the most common security technology examples, but there are some additional tech trends appearing within modern physical security systems technology, including:

Cloud-based surveillance solutions

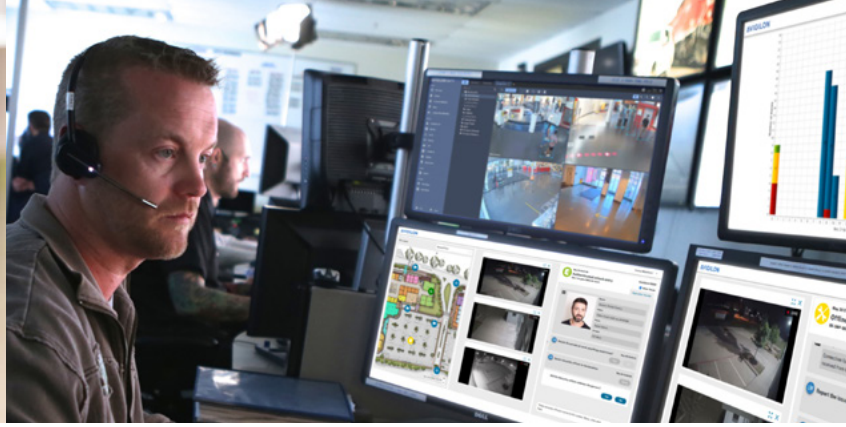
The cloud continues revolutionizing how businesses store and share information. As one of the leading security trends of 2025, cloud computing is facilitating streamlined multi-site management, integrated security technology solutions and enabling fully remote security operations.

As a result, businesses and security teams can access, manage and control their security operations from anywhere at any time. No longer are security operators restricted to monitoring events across their facilities from behind their desks. Teams can carry out their daily duties and monitor on-site activities remotely via video cameras, such as IP dome cameras, and on the go via browsers or mobile devices.

Security managed through the cloud, such as cloud-based video security systems, also extends to maintenance and system availability tasks and is identified as one of the new security technology trends of 2025.

Businesses receive real-time notifications to their mobile devices should a security camera malfunction or a server go down. With this, security teams can ensure that their systems are working to secure and safeguard people, assets and premises.

While cloud security has helped businesses accommodate flexible and hybrid work models, it also comes with risks. As businesses rely more heavily on cloud storage for their security technologies and devices, 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 video cameras equipped with AI analytics. This intelligent technology makes watching live video obsolete. Security systems can accurately detect and identify people, classify 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/vehicle counting and combing through activity logs.

Machine learning continues to be an important component of new information security technology trends of 2025 and can be found in many current license plate recognition systems and video management solutions. By continuously monitoring the network and system configurations for suspicious activity and providing an automated response to any threats detected, security teams can stay informed in real-time of potential incidents. Of the physical security and cybersecurity trends of 2025, this is one to watch closely because the main benefit of machine learning is that the technology only gets faster and more accurate with time.

With the rise of generative AI and language models, such as ChatGPT, AI is firmly in the public spotlight. Businesses must be aware of the cybersecurity and privacy risks associated with such technologies. Camera networks are playgrounds for malicious hackers, and steps must be taken to protect the infrastructure, including encryption, installing the latest software updates and following cybersecurity best practices – one of the key cybersecurity and information security trends of 2025.

Businesses should also not become over-dependent on AI and machine learning to manage their security operations. Human input is still critical to safeguarding valuable assets and people, so security teams must find a balance between the use of AI and machine learning without removing the valuable involvement of a security operator.

Unifying security systems

In recent years, companies have started integrating various security systems with new access control trends to enhance safety and security across their premises. The obvious unification that most businesses are aware of is integrating video surveillance with access control to synchronize footage with access activities at access points so operators can verify events.

However, more integrations exist that can further improve security operations. Powerful connections through an ecosystem of technologies, such as integrating radio with video security and access control, can result in more efficient operations, higher productivity and faster response times to developing threats and incidents. By removing these siloes and bringing them together on a single platform, security teams can simplify management and automate workflows. For example, instead of installing an access reader, a security camera and an intercom device at the front door, all-in-one video door intercom systems now combine all these functions into a single device.

That's why it is crucial to find security solutions that are built on an open platform to allow for such integration across different security platforms – and for cost purposes, too. Open-platform security technology seamlessly integrates with your existing systems, meaning businesses do not need to rip and replace their current hardware, saving them time and money.

Future-proofing through scalable solutions

An additional security and cybersecurity technology trend of 2025 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 are protected against potential cyber-attacks and data breaches. As time elapses and new threats and attack methods develop, security systems must be constantly updated to ensure the latest software and protection features are available to help combat potential threats.

Privacy and data protection

As security technology continues to evolve and its applications multiply, privacy and compliance take on greater importance and will be a crucial addition to the cybersecurity and information security trends of 2025 - particularly when it comes to video. As seen with the U.S. government banning Chinese security cameras and equipment due to national security concerns, organizations are prioritizing procuring video surveillance solutions that meet compliance and privacy requirements.

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 surveillance providers that comply with global government regulations, such as NDAA section 889 compliance and GDPR, and offer security systems built on a cyber-secure platform that is trusted and certified, for example, with the SOC 2 Type II certification. With such technology, it is easier for businesses to ensure that a person's rights are protected while still protecting and safeguarding their people, assets and premises.

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.

How does this impact technology and security for businesses? By understanding how users interact with systems, businesses can quickly identify and remediate any threats before they cause any damage. An advancement from UBA systems that only analyzed user behavior, UEBA systems are an important trend in the 2025 cybersecurity technology industry, offering more complex reporting and greater capacity to spot anomalous behavior based on additional data and improved pattern recognition.

AI video analytics

Over the past year, artificial intelligence has become nothing short of mainstream, and we cannot ignore its implications for the future of security.

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 2025 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 2025 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 2025 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 analytics that can detect and classify objects like people, vehicles and unusual activities 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 security 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.

Intrusion detection system

Avigilon Intrusion detection solution provides a proactive approach to securing facilities by detecting unauthorized access and potential threats before they escalate. This system offers advanced sensors and integration with Avigilon video security, enabling security teams to verify and respond to incidents in real time.

The platform is customizable and scalable, making it adaptable for any facility size or complexity. By integrating intrusion detection with video security and access control, Avigilon delivers a unified security solution that improves response times and minimizes false alarms.

HALO Smart Sensor

The versatile 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 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 vehicles, 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 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**

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.

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

Organizations must be vigilant in protecting their data from an ever-expanding range of threats. Understanding new physical security, cybersecurity and information security technology trends of 2025 is an important step any organization can take in safeguarding its assets. While investing in security technology helps protect people, assets and premises, cybersecurity measures prevent malicious hacking attempts and data breaches.

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 2025 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 cloud-based 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**

MOTOROLA SOLUTIONS

AVIGILON™

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