EBOOK | SECURITY TECHNOLOGY GUIDE

AVIGILON™

SECURITY TECHNOLOGY GUIDE: INDUSTRY TRENDS FOR 2024

Leading trends in physical security and cybersecurity

MOTOROLA SOLUTIONS

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 2024.

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 2024 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 2024, 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 2024 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 2024 point to more robust solutions equipped with AI and machine learning.

The Importance of Information Security Technology

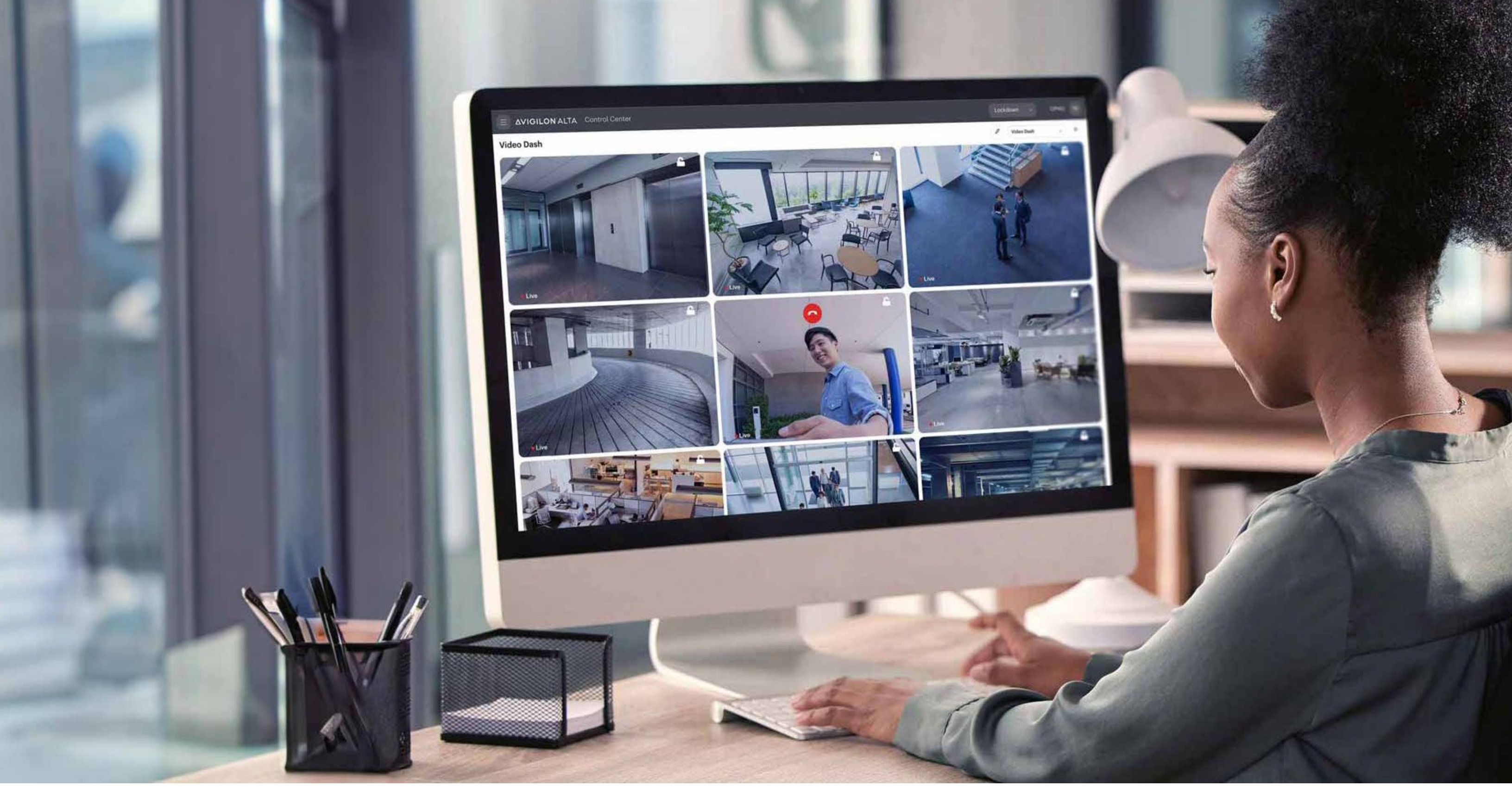
Data security technology and IT security technology are cybersecurity practices and systems that protect information and networks from unauthorized access or disruption. This sector relies on both physical and cybersecurity measures. It is composed of a wide range of system control and protective measures 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 2024?

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 2024 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 2024:

- 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 2024.

TOP SECURITY TECHNOLOGY TRENDS OF 2024

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 2024, 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 2024. 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 2024 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 2024, 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 2024.

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 2024 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.

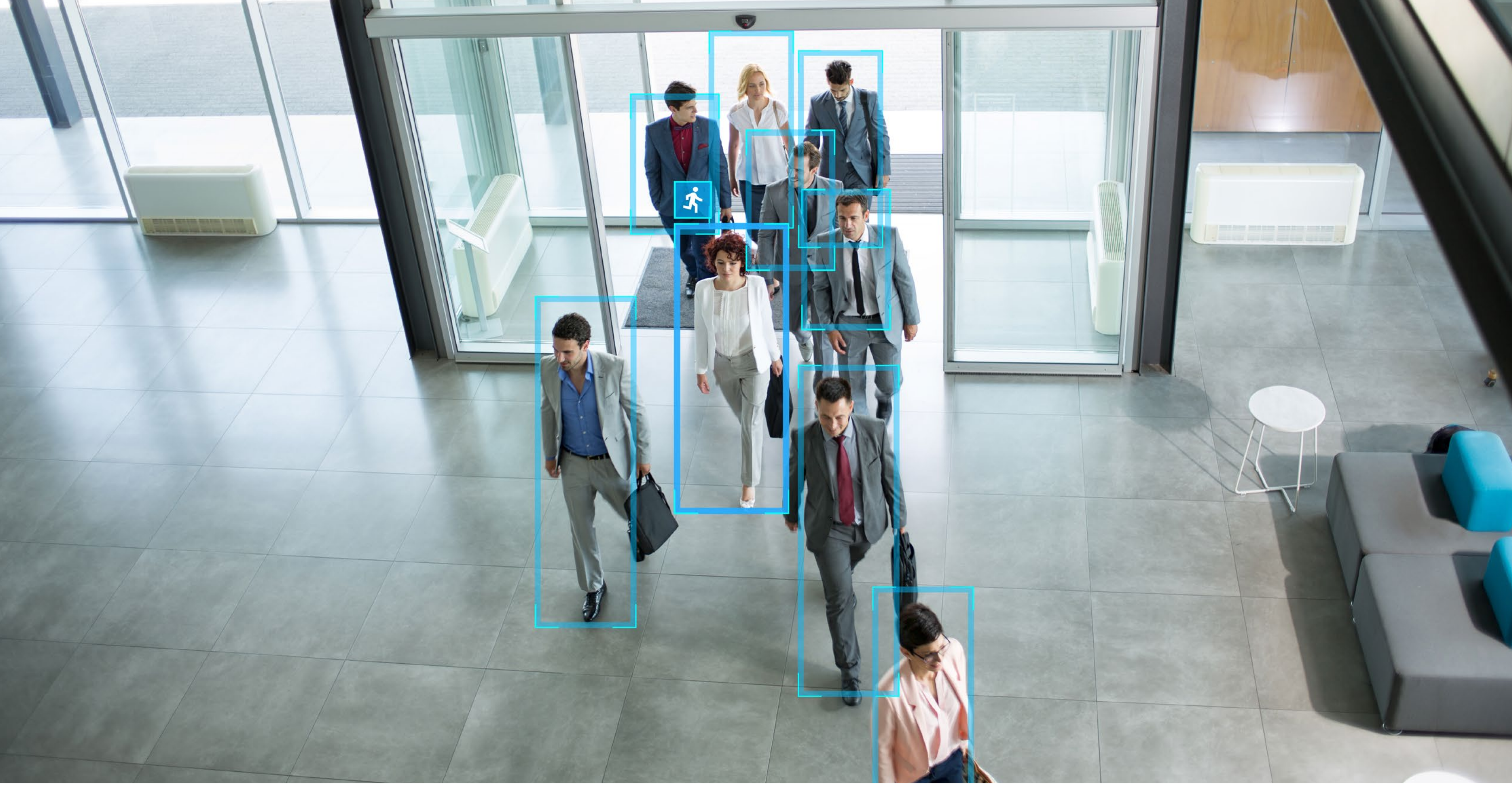
Future-proofing your security systems also ensures they are protected against potential cyber-attacks and data breaches. As time elapses and new threats and attack methods develop, security systems must be constantly updated to ensure the latest software and protection features are available to help 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 2024 - 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 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 2024 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 2024 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 2024 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.

Mobile-first technology

Last, but not least, mobile-first technology is predicted to be a key physical security trend for 2024 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.

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 2024 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 2024 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.

To learn more, visit: **www.avigilon.com**

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