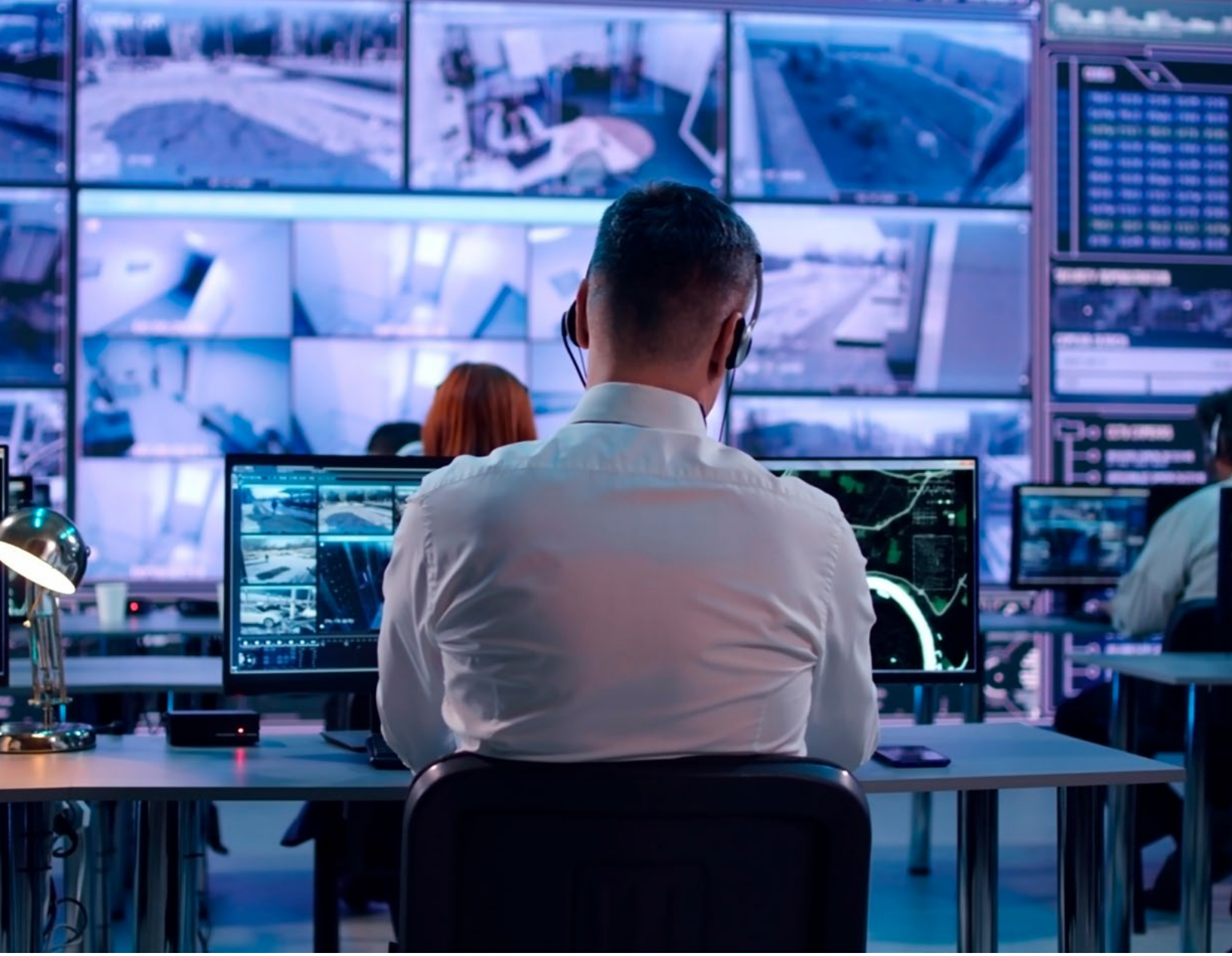
AVIGILON™

SECURITY TECHNOLOGY GUIDE AND TOP TRENDS FOR 2023

Leading trends in physical security and cybersecurity

MOTOROLA SOLUTIONS



SECURITY TECHNOLOGY GUIDE AND TOP TRENDS FOR 2023

No security strategy is complete without the right technology. But choosing the right providers, and staying on top of the latest security technology trends can be overwhelming. In this guide, you'll learn about the different types and components of security technology available today, and how security trends are shaping the way businesses leverage that technology. Plus, see which physical security trends and cybersecurity trends 2023 will bring.

WHAT IS SECURITY TECHNOLOGY?

New developments and ideas continue to shape the future of security technology, and security breach news is a constant reminder of how important the right technology is to success. However, identifying and implementing the latest security technology trends is only effective with a deeper understanding of what security technology is, and how it works. Security technology are concepts, policies, and components designed to minimize risk, identify vulnerabilities, and inform how and when to respond to potential incidents. But good security goes beyond just installing a system.

Physical security

There are four components of security technology that work together to create a holistic system. Let's take a closer look at these four elements that make up a successful strategy, and common security technology examples of each.

- **Deterrence** – These are the security strategies used to minimize the risk of a security breach in the first place. This can be as simple as a physical barrier, such as a fence, gate, or wall. However, implementing the latest security technology can also be a deterrent for both physical and cybersecurity breaches. Video surveillance cameras, IoT enabled commercial door locks, and password protection are all security technology examples that can deter people from attempting to gain unauthorized access to a space or information.
- **Detection** – As often seen in security breach news, being able to quickly identify an incident is key to minimizing the damages done. In that regard, security tech such as access control that can notify teams of a door being forced open, alarm systems, and real-time network monitoring are essential to a complete security strategy.
- **Prevention** – Different from deterrence, this component is designed to delay or slow the progress of a breach or intrusion. Security technology examples that fall under this category include multiple forms of access control, data encryption, multi-factor authentication (one of the top cybersecurity trends).
- **Response** – Security breaches are nearly inevitable. That's why the right technology also helps organizations promptly and accurately respond to incidents. Security technology products including building lockdowns, remote access and controls, and the ability to send live video feeds to first responders are all great examples of this component. No security strategy is complete without the right technology. But choosing the right providers, and staying on top of the latest security technology trends can be overwhelming. In this guide, you'll learn about the different types and components of security technology available today, and how security trends are shaping the way businesses leverage that technology. Plus, see which physical security trends and cybersecurity trends 2023 will bring.

In addition to the above four components, it's also important to note that a security system is only as good as its implementation practices. Even with the top-of-the-line security technology, organizations need to have security concepts and principles in place that define how and when each of the components are used. These methods are key to ensuring all elements of the system are working together to protect people, data, and spaces in a holistic way.

TYPES OF SECURITY TECHNOLOGY

Generally, security technology falls under two main categories: physical security and cybersecurity. While there are some key differences in the design and use cases for these types of security technology, they are both of equal importance. In fact, the best security strategies approach physical and cyber together as a combined effort, also known as security convergence. Understanding the differences between these security technology products, as well as how they work in cohesion to support each other, helps companies better prepare for the future of security.

Physical security

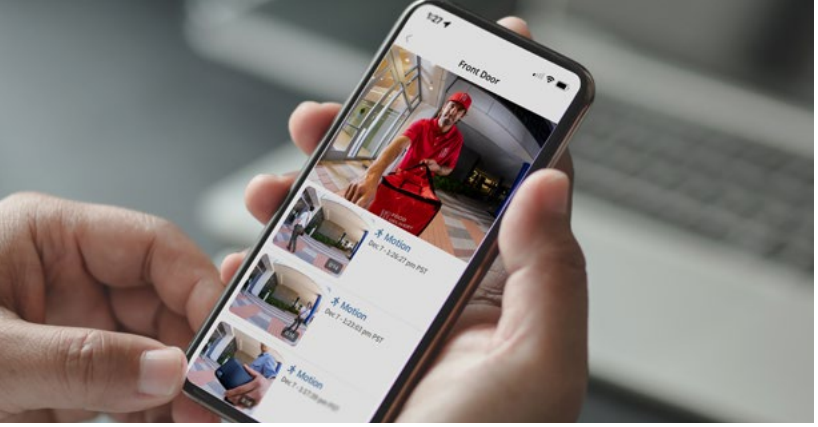
Physical security are methods that protect against physical intrusions or actions within a space, including tools and technology used to monitor physical spaces and people's actions within that environment. The three main components are access control, surveillance, and testing. Some organizations are reluctant to invest in the latest security technology trends for this sector, but physical security plays a key role in protecting data and information, too. With recent innovations and cloud security trends, physical security technology is getting smarter, with new capabilities to connect with other systems and improve incident responses. This interoperability is one reason physical security trends in 2023 point toward technology that leverages cloud-based software and AI.

Cybersecurity

A broad way of speaking about protecting digital assets, cybersecurity refers to strategies that secure information, data, and networks. Cybersecurity, as well as its subsets of infosec and information technology security, are becoming more prominent among security industry trends. Recent security breach news often includes stories of hackers gaining access to confidential information by bypassing cybersecurity controls, or compromising information technology security systems. Because this type of technology is used to protect digital assets from both internal and external threats, every organization needs to know the latest cybersecurity trends if they want to avoid falling victim. Knowing the different types of cybersecurity systems is key to implementing best practices.

WHAT ARE THE 5 TYPES OF CYBERSECURITY?

- **Application security** – This type of cybersecurity technology involves countermeasures to protect software, hardware, and data at the application level. This means that these barriers are coded into the application at the time of creation, such as data encryption. The benefit of this data security technology is that it prevents people from tampering with and modifying software. Additional application security measures, such as rigorous testing and real-time logging, are important to ensure cloud, web and mobile-based applications are protected against the latest vulnerabilities.
- **Cloud security** – A form of cybersecurity for businesses that eliminates physical data retention, this is a leading topic among security industry trends. Cloud computing is great for storing large amounts of data, which takes the burden off organizations to manage and maintain local servers. Because the cloud is accessed and often managed remotely, the future of security technology involves finding innovative ways to limit access, and utilizing multiple cybersecurity systems together. In this regard, new cloud security trends include synching identity providers in the cloud, better access management through the principle of least privilege, and centralizing logging and monitoring for a more complete understanding of traffic across your networks.
- **Endpoint security** – As IoT-connected devices become more prevalent, information technology security at the device level will continue to be an important cybersecurity strategy. Endpoint protection examines files as they enter the network, such as when a user logs in on their smartphone or laptop, or when a file is sent to a printer. Active endpoint monitoring technology can help organizations spot vulnerabilities by detecting and alerting to unauthorized logins, phishing attempts, viruses, and malware.
- **Internet security** – With so many devices connecting to the Internet in the workplace, cybersecurity is more important than ever. This type of data security technology limits who can access certain websites, and monitors the information sent and received through browsers, alerting to any potential unauthorized use. Most browsers have built-in Internet security measures designed to protect everyday users. Many organizations also implement additional Internet security measures, with firewalls and multi-factor authentication (MFA) being the top cybersecurity trends in this space.
- **Network security** – The function of network security is to prevent access and use of information and data through the local network connections. This type of cybersecurity technology helps protect the organization's IT infrastructure by ensuring logins, passwords, and access to the local Internet connection remains secure. Antivirus software, data encryption, and intrusion detection systems are all common methods of network security.



CLOUD VS. ON-PREMISE SECURITY TECHNOLOGY

Choosing the right security system is an important decision, and often a big investment for any size organization. There are two types of systems, with key differences to note: cloud-based and on-premise. What are the latest security technologies, and which one is right for your business?

The main differentiator here is where these systems are managed. On-premise security tech runs on locally managed servers at the building site, and is viewed as the more traditional, or "legacy" option. With cloud-based systems, the servers are managed by a third-party, with local data synced via the cloud. Most cloud security tech providers use Amazon Web Services, Google Cloud, and Microsoft Azure for their server management. Take a closer look at how to compare cloud-based and on-premise security technology, and select the providers that are right for your business.

Reasons to choose on-premise security systems:

- On-premise uses thick client software which offers greater customization capabilities
- Management software can be browser-based or tied to a specific on-site workstation
- Good option for high-security environments with strict policy or compliance requirements
- Installation, maintenance, and updates are all performed by a trained, on-site IT professional who knows the specific system
- Compatibility with existing on-premise security systems Get your free security consultation

Reasons to choose cloud-based security systems:

- Eliminates the need to invest in on-site hardware and IT management
- Scales with ease thanks to fully remote management capabilities and no server hardware to install on location
- Software updates are automatically installed over the cloud
- New capabilities and features are easier and faster to roll out across all sites
- Redundancies built into large data centers increases cloud system reliability
- Cloud security technology is often built on open standards for easy integration with other systems

What if an organization has an existing on-premise security system, but also wants access to some of the capabilities of a cloud-based system? Luckily, there are cloud-based security systems that are backward compatible with legacy technology. In a hybrid model, organizations can retain their original investment in on-premise servers, and upgrade the edge devices to cloud-based technology. For example, an organization that wants to keep their original on-premise ACU hardware can choose to update their door readers with a cloud-based access control system provider, allowing them to take advantage of frictionless mobile-based credentials and remote management without having to rip-and-replace the entire system.

TOP 8 SECURITY TRENDS 2023

The latest security industry trends are constantly evolving in response to an ever-changing list of vulnerabilities and threats. Even as technology gets smarter and more connected, organizations that are actively monitoring the latest security technology trends are more prepared to face new challenges. See which physical security trends and cybersecurity trends are the ones to watch in 2023.

1. Adopting MACH architecture for the enterprise

One of the biggest buzzwords in security trends right now is MACH architecture, which stands for Microservices, APIfirst, Cloud-native SaaS, and Headless architecture. Rather than building your entire system on all-in-one, monolithic architecture, MACH architecture instead relies on choosing best-of-breed providers, and connecting them via an open API platform. Popular among companies looking to deploy modular, customized systems with less development time, many see this as the future of security technology for enterprise organizations. There are three main reasons to migrate to MACH architecture for security technology: leveraging an open API to choose the best providers for each system element, the interoperability of a customized solution, and automatic updates that get rolled out to each component as soon as they are available. With security tech that's built on open, cloudnative standards, organizations have the ability to connect any other building system they need: video surveillance, alarm systems, tenant apps, and even completely custom solutions. The result is a connected, high tech commercial security system that's responsive to the needs of that specific organization, with increased operational efficiency. The highly modularized architecture gives businesses access to more innovation, greater flexibility to build the solutions they need, and better adaptability to face the future of security as needs continue to evolve.

2. More mobile-first management

The migration to remote and hybrid work models has emphasized the need for more mobile solutions. As a result, one of the biggest physical technology trends will be the continued development of mobile experiences for keyless door entry access and management. Tomorrow's technology won't just be a mirror of the desktop experience, either. The frontrunners are designing uniquely for the mobile user. While many innovations last year focused primarily on the end user, it's expected that security trends 2023 will focus more heavily on the management side of the equation. Organizations need to know what's happening in their spaces at any given time without physically being there. When real-time video surveillance, access logs, and building system data are all just a tap away, it's easier to make decisions and respond quickly to potential incidents. Taking these security concepts and principles a step further, options to unlock the door, turn on the lights, or notify first responders within the same mobile platform has the potential to significantly increase efficiency and improve security posture for any size organization.

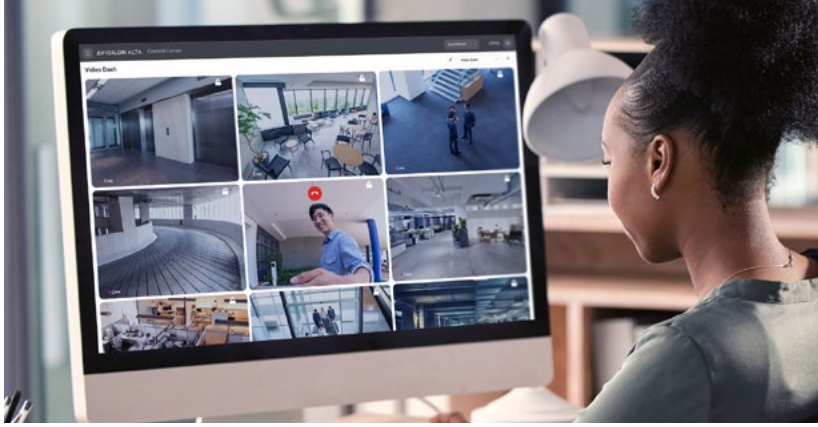
The future of access control and security will make communication, controls, and data easily accessible on a mobile device, without compromising on security.

3. Security convergence powered by AI

Holistic security concepts and principles continue to dominate the market. Security industry trends that merge physical and cybersecurity strategies give organizations better visibility and more control, so it's no surprise that convergence still makes the list for security trends in 2023. However, the approach to security convergence is shifting. Now, the interconnectivity of the threats across every component of security systems also must be addressed. Organizations need to establish a multi-factored security strategy with consistent vulnerability testing, granular access, and automatic system updates. Leveraging AI to help teams identify incidents and provide enhanced focus is a smart way to implement the latest security technology for successful convergence. AI isn't going anywhere, and while adoption is often slow, AI is an important tool in establishing more adaptable and responsive systems and teams, and enterprises looking for more effective security convergence strategies should take note.

4. Remote access to everything, anywhere

When people depend on their technology for just about everything, remote access is no longer a nice-to-have capability. As organizations continue to refine their strategies for accommodating a remote workforce, the ability to know and respond in real-time, from anywhere, becomes more crucial than ever before. The cloud is getting more powerful and more secure, making it a promising advantage for remote security management. Especially for enterprise and multi-site organizations, remote management will define the future of security technology, becoming an essential part of every business strategy. Today's technology is built to be more intuitive and collaborative, giving businesses stronger insights into trends across all their sites and locations. Now, it's possible to grant employee access, track and see when deliveries are made, manage lighting and HVAC systems, and monitor office occupancy – from anywhere in the world. The key differentiator to look for in a leading access control provider jumping on these security trends? Those that maximize interoperability and centralize all that data into a single dashboard, with a single login. Security Technology Guide



5. Combining (and scaling) video and access

One of the most important security trends 2023 we'll see is the merging of video surveillance and access control. Powered by effortless cloud-to-cloud integrations, and the physical security trend of adding video cameras to door readers, modern video access control systems make it easier to associate visuals with access events. Traditional video surveillance isn't going anywhere. In fact, the growth of the cloud and IoT technologies means now businesses can leverage their existing security cameras and hardware by connecting them to their access systems. Together, business security camera systems and access control provide a more complete picture of what's happening at any given moment, from the front door to high-security interior spaces. One challenge that these security trends address is the ability to scale these technologies. Before, organizations would need to install and wire a new camera in every space into which they wanted visibility. Plus, cloud-based management allows organizations to scale their security monitoring in a cost-effective manner, eliminating the need to have on-site staff at each location 24/7. As part of MACH architecture security trends, organizations can also choose interoperable video and access providers to build a more custom solution to fit their needs, and no longer need to settle for a one-size-fits-all provider.

6. 5G and AI technology's impact on cybersecurity trends

As 5G makes its way into the mainstream, businesses need to be prepared for a new string of cybersecurity risks. 5G has huge potential for the IoT-connected world, as faster, more powerful connections become possible across more devices. This new network availability, however, will require more advanced security technology, with stringent activity monitoring and threat detection software. Machine learning and AI have proved effective for automating threat detection technology to improve cybersecurity. When there are hundreds or thousands of events occurring on your network every minute, AI threat detection helps security teams flag issues. Time is of the essence during any cybersecurity incident, and smarter data security technology can help minimize potential exposure. While the predictive elements of this cybersecurity technology is still not foolproof, AI-powered systems show great potential. From utilizing smart detection for occupancy counting in parking lots, to identifying and notifying security teams of unauthorized network activity, AI is one of the leading cybersecurity technology trends to watch in 2023.

7. Supply chain disruption

One of the newest security technology trends is innovation within the supply chain. Supply chain incidents reported in security breach news have revealed that when one system in the chain is compromised, it often causes issues for the entire network. Supply chain disruptions are affecting every industry all over the world, so organizations everywhere are looking for new security technology for loss prevention. Leveraging security tech that can better protect networks, identify potential security incidents, and monitor product movement in real-time will be key to safer supply chains in 2023.

8. High tech security as an amenity

While security may not be the first thing that comes to mind when you think of building amenities, it's a top technology trend in real estate. Both commercial and multi-family residential real estate are seeing increased interest in advanced security technology among tenants. Taking a more modern approach and investing in the latest security technology gives tenants peace of mind that their space is secure, and shows that their landlords are paying attention to new security trends. Touchless access, digital tenant apps, and smart video security are all top trends in physical security, while 5G, better network monitoring, and remote connectivity are cybersecurity trends tenants will be looking for in 2023. However, more security isn't always the answer. The end-user and customer experience still matters, so providing flexible access methods such as key cards and fobs alongside mobile based credentials are still important. Convenience is king when considering physical security as an amenity, so navigating new security systems should still be intuitive and frictionless at every touchpoint.

Key takeaways

Looking at the top security trends in 2023, it's clear that adaptive technology is where the industry is headed. The future of security technology will rely heavily on new ways to centralize data and automate operations. Cloud-based systems, AI-powered software, and stronger IoT connections are all key to navigating the new security landscape. As organizations seek new ways to make workplaces more efficient and support a sustainable hybrid work model, the right security technology will play a crucial role in being able to quickly adapt to the needs of tenants and employees, as well as protect data and information from a host of new cybersecurity threats.

To learn more, visit:
www.avigilon.com

MOTOROLA SOLUTIONS

AVIGILON™

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