

PELCO[®]

Physical security: key controls, policies and examples



Complete guide

Physical security planning can feel daunting, and it is difficult to know where to start. Now, many companies focus efforts on cybersecurity – after all, modern businesses rely heavily on their data and IT infrastructure for day-to-day activities.

However, physical security plans should be equally high on the agenda. Striking a balance between digital and physical security measures helps protect your business from all angles, safeguards your reputation and makes your employees feel safe at work.

This guide outlines security fundamentals, including the most common threats, prevention measures and technologies. It also provides helpful information on applying these fundamentals to your company and a handy step-by-step process to help you start your physical security plan.



What is physical security?

Physical security is the protection of people, property, data and assets from physical actions that can cause damage or loss. This includes the prevention of theft, vandalism, accidental damage and natural elements that can harm an establishment.

Physical security is often referred to as just being “guards and gates”, but modern systems consist of a variety of elements and measures, including:

- **Site layout and security configuration:** Identifying weak points and determining what needs protection.
- **Visibility of critical areas:** Using security cameras and lighting to observe activities in essential areas.
- **Staff training:** Ensuring employees know how to handle incidents and establishing an emergency response process.
- **Perimeter protection:** The traditional “guards and gates” aspect of physical security.
- **Access control:** Securing a site using simple locks, keypads or biometric access readers.
- **Intrusion detection:** Using video security, motion sensors and tripwire alarms to detect unauthorized access.

As you can see, the examples above vary, touching on different aspects of a site and its functions. Some physical security plans are determined by environmental factors, such as your site layout while some are behavioral, such as staff training.

Successful protection of people, property and assets involves a comprehensive range of security measures, including the protection of equipment and technology like data storage, servers and employee computers.





Physical security measures and methods

Before using any physical security solution, you should understand how different elements combine to contribute to your overall plan. The main types of physical security fall into four broad categories: Deter, Detect, Delay and Respond.

These four security methods work together in a layered approach to help protect your people, property and assets. The levels of physical security begin with Deter at the outermost level, working inwards until finally, if all other levels are breached, a Response is needed.

Deter

Deterrence physical security measures are focused on keeping intruders out of the secured area. Common methods include tall perimeter fences, barbed wire, clear signs stating that the site has active security, commercial security cameras and access controls. All of these are designed to give a clear message to criminals that trespassing is not only difficult, it is also highly likely that they will be caught.

Detect

Detection works to catch intruders who get past the deterrence measures. Some criminals might slip in behind an employee - known as tailgating - or find a way of scaling barriers. A physical security measure that can detect their presence quickly is crucial in these cases.

These include many types of security systems that you are likely familiar with. Examples include security cameras, artificial intelligence (AI) video analytics, motion sensors

and intruder alarms. If an intruder is spotted quickly, it's much easier for security staff to stop the security threat from developing into a critical incident and contact law enforcement for assistance.

Delay

Delaying an intruder or other security threat helps protect a business's people, assets and premises. Access control systems requiring credentials to open a locked door help slow the progress of threats and give security teams the time to locate the threat and initiate a response to remove it efficiently.

Respond

Having the technology and processes to respond to intruders and take action is crucial for physical security, yet often overlooked. Response physical security measures include communication systems, security guards, designated first responders and processes for locking down a site and alerting law enforcement.

Physical security control technology

There are several tools and cutting-edge technology within the four main types of physical security control categories and, in recent years, they have evolved in leaps and bounds, offering advanced protection at accessible price points. Several security devices now use cloud technology and AI for even more flexible, smarter real-time processing.

Additionally, security technology is now more scalable, so you can implement it faster on demand, and provide insightful data for audit trails and analysis. It is also useful for demonstrating the merits of your physical security plan to stakeholders.

Consider how different security solutions will work together when scoping out your physical security plan. Devices that seamlessly integrate will help enhance your overall security operations by providing increased awareness, efficient threat detection and automated decision-making. Universal standards, like ONVIF, enable devices from different manufacturers to integrate more smoothly than before.

Video security

Security camera technology is a core element of many physical security plans today. Primarily a detection form of technology, video security cameras continuously record activity in an observed space, enabling security teams and managers to see what's happening in real time or view recorded footage later. Users can view the footage to provide the awareness needed to help secure their facility, safeguard people and initiate investigations.

Security cameras have advanced significantly from recording analog signals to tape. So too has internet connectivity – thanks to fast network connections and the cloud, transmitting and accessing high-quality video is quicker and easier than ever before. With AI analytics technology, security cameras can help you automatically spot suspicious activity in real time. They can also be used to deter intruders since the sight of cameras can discourage criminals from attempting to commit a crime.

Internet protocol (IP) cameras use the latest technology to transmit high-quality video over an internet connection. These cameras have many smart features, from built-in AI analytics and microphones to low-light capabilities, that enhance security operations and performance. With many different IP camera types, you should consider which one suits your particular security application or environment.

As the name suggests, fixed IP cameras have a fixed viewpoint. This might sound limiting, but most cameras only

need to focus on one key area at a time. Fixed IP cameras are a great choice for indoor and outdoor use, and there are models for both. These cameras can handle poor lighting conditions and come in three form factors, bullet, dome and box, providing reliable and comprehensive coverage.

If 360-degree outdoor views are what you need, then pan-tilt-zoom (PTZ) security cameras are the perfect choice. These give you ultimate control over what you can see in a certain area as you can adjust the camera's view remotely. They are made to be versatile in a range of lighting conditions, with long-distance views. Also, PTZ cameras tend to have strong enclosures that protect from different weather and environmental conditions so be sure to seek such capabilities and certification if you're seeking a robust device.

If you want 360-degree views inside your premises, panoramic IP cameras, such as the fisheye and multi-sensor, are a great option. They capture video from all angles, making them ideal for observing large indoor environments.

Additionally, license plate recognition (LPR) cameras are used by law enforcement, parking lot operators and city safety teams to capture vehicular license plate information to identify any vehicles involved in known crimes or are on the watch list.





Access control

Access control technology is another cornerstone of physical security systems that help secure premises and protect the people and assets inside. Like video security, access control systems give you an overview of who is entering and exiting your premises. It also gives you physical controls to keep certain people out and authorize people to enter.

Access control systems can help detect and delay intruders from entering. They can also deter intruders by making it too difficult to attempt entry. As with security cameras, there are many different types of access control devices.

Keyless access control relies on modern methods of authentication to authorize entry. One example of this is mobile access control. Now, employees and visitors can use their smartphones to verify themselves. In addition to being easy to use, keyless access control removes the risk of lost or duplicated keys and keycards, mitigating potential associated security risks.

Many access control units now also include two-way video. This provides an added layer of verification so authorized individuals can check who is attempting to enter. These security devices have the added benefit of using smart technology that connects to the cloud or a web interface. This allows you to observe and control your entry points remotely and provides valuable data to help you with building management.

AI analytics

Physical security technologies can log large quantities of data around the clock. Now, this information can be enhanced with smart analytics. AI-powered analytics can process all this data and provide helpful digests for your security team, saving them valuable time and helping them make faster, better-informed decisions. Many types of physical security technology feature AI analytics as part of their core functionality; however many options are available for a more tailored setup.

Analytics platforms and capabilities are extremely varied and there are now options for many physical security tools. For example, smart video analytics, like LPR, can identify relevant activity such as vehicles, while filtering out false alerts that can waste time. Analytics can also compile summaries of incidents and generate reports of the data you want to investigate, whether this is the number of alerts over time or the performance of your physical security device.

These insights are highly valuable for business operations and compliance. Many companies have physical security policies that require comprehensive reporting and audit trails. Analytics can help provide this information in an accessible format and simplify the overall compliance process for security staff. Activity and performance data offer valuable insights for operations; by looking at how your physical security plan works over time, you are much better informed on how to improve it.



Sensor technology

Sensor technology is another detect form of physical security and a key element in your security setup. These smart building devices detect environmental changes and alert security teams to threats like break-ins, poor air quality or smoking. The most common type of sensor is a smoke alarm, which helps to indicate a fire. However, multifunctional devices on the market today help detect and observe several aspects of health, safety and security, including motion, sounds, light, vaping, temperature and more.

Upon detecting vape, loud noises, unusual motion or other triggers, the sensor will notify the operator and enable the security team to respond quickly. When integrated with the wider physical security setup, the operator can use their security cameras to gain greater visibility of the incident and initiate a lockdown via the access control system, if necessary. These quick alerts, automated decision-making and fast responses can help to extinguish the threat and restore a safe environment.

Sensor technology is a great security tool for privacy-concern areas, such as washrooms and changing facilities, where video and audio recording are prohibited. For example, in schools, vaping and fighting incidents often occur in these spaces, away from security cameras and the presence of school staff, and sensor technology gives organizations a level of observation.

As there are multiple elements that organizations will want to detect and observe in privacy-sensitive spaces, it is important to consider what types of specific sensors will be needed. Multiple sensor types may need to be installed and wired, or organizations may choose to implement a modern all-in-one [Halo Smart Sensor](#) that can detect a plethora of threats.

Methods to identify physical security threats

Conducting a thorough [physical security risk assessment](#) is the best way to uncover potential weak spots. Stress testing physical security rigorously will reveal where your main challenges are. Identifying these existing vulnerabilities will help you address them in your physical security investment plan. You can conduct this risk assessment yourself or consult a specialist physical security company to do it for you.

Physical security failures are not always the direct result of a poor physical security system. Sometimes, even with many of the right physical security measures, problems can arise because of weaknesses or challenges in other business areas. Some of these challenges are not obvious but will require stress testing or investigations to reveal them.

Examples of physical security challenges

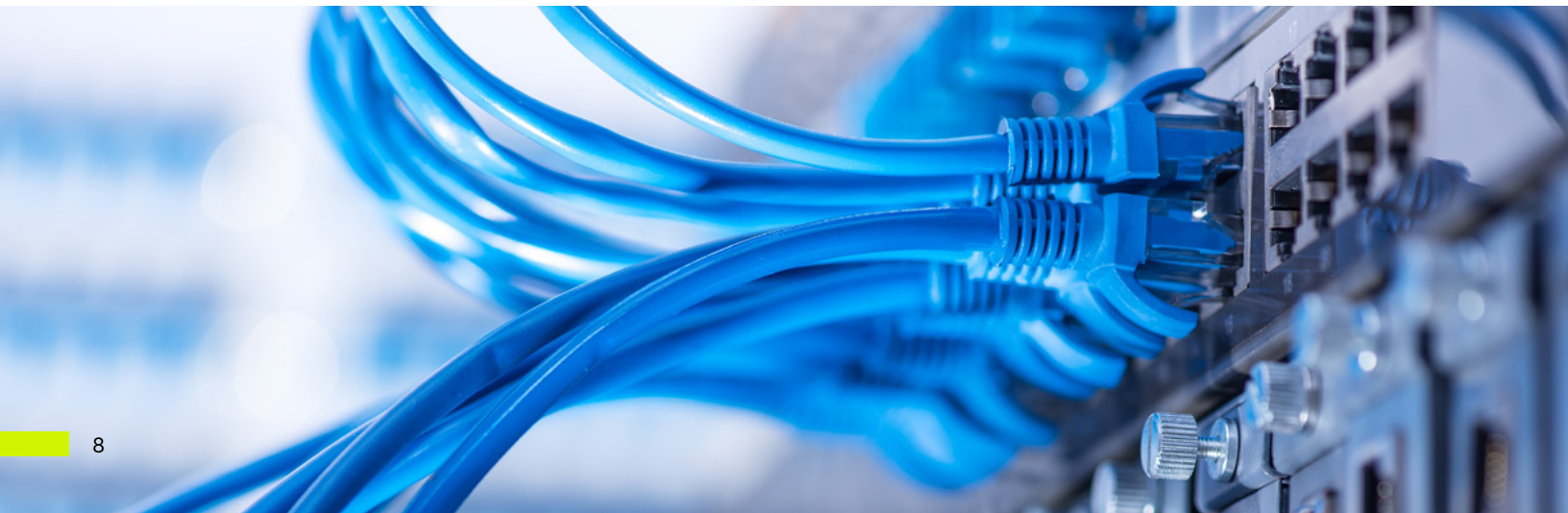
Budget shortages: Small or restricted budgets can prevent many businesses from making an appropriate physical security investment. However, failing to budget for an adequate physical security system can lead to security failures over time, leading to greater costs. Some security measures can strain a budget more than others; for example, hiring security guards can be costly, especially if many are needed to guard a site for long periods. In addition, more advanced physical security hardware, such as top-of-the-line security cameras and access control systems, will inevitably be more expensive. However, not having those measures in place can expose a business to many physical security threats, which can be just as costly and risk the business' health.

Staff shortages: Not employing enough staff can impact physical security systems. Even with the most advanced physical security technology, businesses still need personnel to oversee larger systems and make decisions. In the wake of the coronavirus pandemic, businesses suffered from recruitment shortages. Not having enough people to implement your physical security plan can strain morale and cause operational issues. Even if you can recruit new staff members, if they are not sufficiently trained in the technology you use, or aware of company security policies, then this can also create bottlenecks that expose you to greater risk.

Inadequate security technology: If your technology is not properly integrated into a larger physical security system, it can bring problems rather than benefits. A key factor is how your security devices interface and how they feed information into your system. If your devices are not compatible or properly integrated, critical information might be missed, such as break-ins. One way to minimize the likelihood of this happening is to use devices that comply with ONVIF standards. ONVIF is a set of standards designed to enable different types of physical security technology to integrate seamlessly, regardless of manufacturer.

Too many sites to manage: Securing multiple connected sites involves keeping track of many moving parts. No two sites are the same, so in addition to implementing a company-wide physical security policy, your plan must be flexible enough to accommodate each site's unique security threats and vulnerabilities.

Lack of coverage: Comprehensive coverage of your sites is difficult to achieve with video security cameras, access control and onsite guards alone. Within facilities, there are multiple spaces and rooms where video and audio recordings are not allowed, and so is the presence of security guards. Areas like hotel rooms, restrooms and changing facilities are environments where the user's privacy must be respected. However, physical security threats and incidents can still occur in these spaces. Smart sensors with non-invasive security features can be leveraged to help ensure comprehensive security insight in all areas.





Common physical security threats

Each business's physical security risks will be different, but there are some common threats to be aware of.

Unauthorized entry: This includes tailgating, social engineering or access via stolen passes or codes. The earliest physical security breaches are, logically, at the first entry point to your site. If unwanted visitors manage to gain access, then it is only a matter of time before other physical security threats can occur.

Theft and burglary: Businesses own many valuable assets, from equipment to documents and employee IDs. Some businesses are extremely exposed to theft because of the expensive assets they store on their premises, while others may store valuable data that may attract some thieves. However, you also need to be aware of thieves from within the business as employees tend to have easier access to commit theft. The National Retail Federation found that internal theft accounted for 28.5% of shrinkage, just behind the leading source, external theft, at 37%.

Vandalism: Some businesses are at risk of their property being destroyed or tampered with. This can be linked to a company's location. For example, if your business is next to a bar or nightclub, alcohol-related vandalism could be a frequent problem. Vandalism can also be ideologically motivated, for example, when activists cause physical damage to a premises by smashing windows or throwing paint.

Violence: Acts of aggression and altercations can be a serious concern to the security of an establishment and the safety of the people within. Fighting, harassment and acts of targeted violence are all physical security threats that are becoming increasingly common concerns in today's security landscape.

Natural disasters: Damage caused by natural causes, including earthquakes, floods and forest fires, can be unpredictable and difficult to defend against. As a result, your workers and assets are exposed to dangers in addition to property damage. This can severely impact your business' operations and future success which is why proper training and security emergency planning are crucial to limiting the impact.

These are a few high-level types of physical security threats. As you conduct a risk assessment of your business, you will discover physical security risks specific to your industry and location.



The rise in cybersecurity threats

As the world embraces and relies even more heavily on digital technology to improve lives, perform operations and expedite human actions, threats from [cyberspace](#) are rising at alarming rates. From extensive data breaches to the hacking of accounts, these cyber attacks have disrupted normal business operations and even crippled some as a result of the financial and reputational damage caused.

As a result, businesses and organizations are now putting greater emphasis on implementing cybersecure physical security solutions to protect against digital threats. Additionally, following good cybersecurity hygiene and training employees on best practices is another focus for organizations looking to reduce the risk of cyber attacks affecting their operations. In the absence of such planning and use of cybersecure technology, businesses and organizations are extremely vulnerable to attacks.

Physical security planning

Drawing up physical security plans requires input from around your business. Physical security measures do not happen in a vacuum - they affect every aspect of your day-to-day operations. Many physical security examples in the guide below also feed into your company's finances, regulatory status and operations.

A good practice for physical security planning is well-researched, holistic and encompasses all your departments and functions. In the following 5-step guide, you will learn how to apply physical security best practices at every stage of your physical security plan, from risk assessment to implementation.

1. Conducting a risk assessment

You cannot approve any physical security investment without knowing which measures are needed. This is why a thorough risk assessment is an invaluable asset – once you have it, you can return to it, add to it and use it to adapt your physical security systems over time.

It might be overwhelming to know where to begin. If you do not have the know-how or bandwidth to do this yourself, many physical security companies specialize in risk assessments and penetration testing. You can also hire a physical security company to consult on the process, guiding you on how to carry it out effectively.

Begin by considering your most common physical security threats and vulnerabilities. Using the Deter-Detect-Delay-Respond categories, think about which physical security breaches might happen in your business at each stage. The most obvious starting point is identifying any unprotected points of entry and areas of interest or high value.

Next, see if your company has records of any previous security breaches. Your insurance will have records of past

claims and prior security management might have kept a log of past incidents. This is also the point at which you should liaise with stakeholders and different departments; the risk assessment stage is when expectations are set and teams' cooperation is required for the overall success of your project.

Investigate your site. Leave no stone unturned and consider that not all physical security measures require cameras, locks or guards. For example, poorly lit areas might need cameras, but improving the lighting conditions will make an enormous difference in how attractive that area would be to criminals. Also, look at low and high-traffic areas; both are prone to intrusion since criminals can slip unnoticed in a crowd or when nobody is around. These are areas where detecting and delaying intruders will be the most important.

Finally, with this information, you can map out where to position physical security components and redundancy networks. A redundancy network is crucial as any physical security control is at risk of not working. In these cases, a backup network will protect you from security threats.





2. Review your operations and resources

All the information you have gained from your risk assessment will help you to ascertain the physical security controls you can purchase and implement. The scale of your project will depend on the resources that are already available. For example, check if you have sufficient internet bandwidth to handle extra IP cameras and smart access controls. You will also need to check you have enough server space to store all the data these physical security devices will generate.

There is then the question of whether you choose to monitor your security in-house or whether you plan to outsource it to a physical security company. One basic consideration is space – do you have enough space on-site for a security operations center? You will also need to consider whether your existing team can handle additional information streams from more devices or whether you would need to recruit more staff. Outsourcing this function can relieve some of the operational pressure, but depending on your industry, you must check whether security policies and compliance require you to keep data confidential.

This is the stage to brainstorm what physical security tools you want, what you need immediately and what your physical security plans are for the mid to long-term. With a thorough plan, it will be easier to work with stakeholders on financial approval.

3. Commercial and operational approval

At this point, you will submit your plan for business approval. The key objective during this phase is to agree on a financially viable plan that does not compromise physical security and leave you open to risk.

As stakeholders and other interested parties scrutinize your plan and suggest changes, ensure you draw up a new risk matrix for each iteration. This way you can refer back to previous versions to check that no security threats go under the radar. Documenting every stage in writing will ensure that you and your stakeholders are on the same page so that there is accountability for how your physical security systems perform.

Be prepared for a situation where you will have to compromise. In these circumstances, review the areas where you cannot devote as many resources as you would like and see if there is a workaround. For example, a seemingly vulnerable dark area might not require specialist thermal security cameras if the lighting conditions are improved. Or, instead of hiring a large team of operators to field alarms, you could see if your current team can handle the extra workload with the help of smart analytics.

4. Implementing physical security policies and setup

All the information you have gained from your risk assessment will help you to ascertain the physical security controls you can purchase and implement. The scale of your project will depend on the resources that are already available. For example, check if you have sufficient internet bandwidth to handle extra IP cameras and smart access controls. You will also need to check you have enough server space to store all the data these physical security devices will generate.

There is then the question of whether you choose to monitor your security in-house or whether you plan to outsource it to a physical security company. One basic consideration is space – do you have enough space on-site for a security operations center? You will also need to consider whether your existing team can handle additional information streams from more devices or whether you would need to recruit more staff. Outsourcing this function can relieve some of the operational pressure, but depending on your industry, you must check whether security policies and compliance require you to keep data confidential.

This is the stage to brainstorm what physical security tools you want, what you need immediately and what your physical security plans are for the mid to long-term. With a thorough plan, it will be easier to work with stakeholders on financial approval.

5. Physical security best practices

As your physical security system beds in and grows over time, there are some best practices to maintain. The cornerstone of your evolving plan should be accountability: who is responsible for every aspect of your company's physical security? To this end, create a security guide or playbook, which everyone can refer to and adapt.

- A list of all the components you use (e.g. cameras, keypads and passcodes)
- A corresponding list of all your device configurations
- Agreed objectives and how to implement them
- Redundancy network protocols and configurations
- Physical security policies for regular testing and maintenance
- Any local, national or international physical security standards or regulations you follow, along with dates for renewal

Having a guide like this keeps all parties on the same page and is a great resource for any new hires. By keeping all your core information together, you will not leave yourself open to any physical security risks or compliance issues.





Physical security planning

Pelco is a powerful devices brand that has set the standard for performance and versatility over the last 60 years. With purpose-built, customizable cameras and sensors for every need, our devices are designed for any situation or requirement and work with the software you already have.

Founded in 1957, Pelco is a trusted video technology partner with a widespread global presence, built on a legacy of delivering high-quality, specialized security products and systems. Across a wide span of industries, loyal customers and partners turn to Pelco as a provider of video technology designed to propel faster deployments, higher levels of system resilience and a lower total cost of ownership.

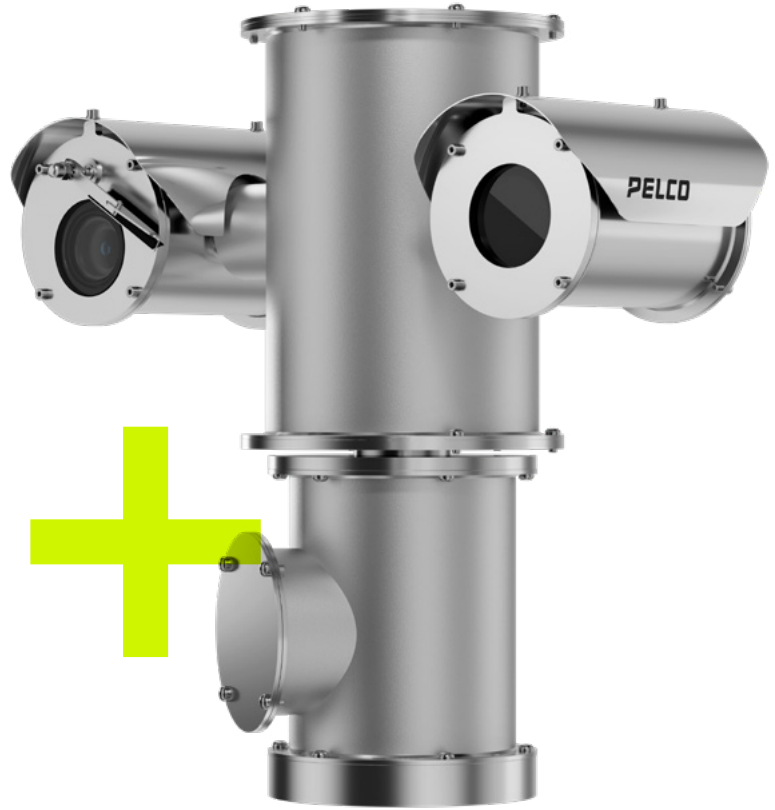
Video security

With customizable cameras for every need, our devices are designed for any situation and built to work with your existing [security systems](#). From budget-friendly bullet and dome cameras to heavy-duty PTZ cameras, Pelco's expansive portfolio of security cameras is combined with powerful AI video analytics that helps transform your security operations so you can stay one step ahead of potential threats.

Whether you're a retail store looking to improve coverage across your shop floor, parking lot and stock rooms or a hospital looking to safeguard staff and patients, Pelco's AI-enabled and ONVIF conformant devices deliver greater safety and security, from the latest Sarix and Spectra Enhanced Series to the hardened Esprit and ExSite lines.

Couple that with Elevate, Pelco's direct camera-to-cloud technology that combines edge and cloud AI, and you can extract more from your cameras to help maximize productivity and efficiency through image health reports, automatic camera updates and more.

[See video security products](#)



Smart sensor technology

Maintaining the safety of individuals and organizations is essential, including where video and audio recording is not permitted due to privacy concerns. These areas pose a unique security challenge as they are often targeted to engage in prohibited or unsafe activities. So, how do you help keep every area of a building safe?

The all-in-one [Halo Smart Sensor](#) is an intelligent device that helps keep buildings safe by accurately detecting vaping, health and safety events. Not only does the device help maintain the safety of privacy rooms by not using video or audio recording, but it also can detect air quality and anomalies that go unnoticed by security cameras. With 12 individual sensors observing vape, health and safety events, security and building management teams can respond rapidly to potential threats and incidents via real-time site-specific notifications.

[Explore Halo Smart Sensor](#)

Case studies

Find out how businesses and organizations have used Pelco's physical security technologies to enhance safety and security and improve overall operations.



Video security for an engineering marvel

With thousands of motorists using the Chesapeake Bay Bridge-Tunnel (CBBT) daily, the operations team must keep track of what is happening across the complex to ensure a safe and efficient journey for all. However, with so many things to look out for, including traffic, incidents and weather conditions, it can be challenging to stay at the forefront of security. As a result, CBBT understood that they needed a system that could provide them with crystal-clear, real-time video of what was happening across the facility.

CBBT deployed Pelco's video security system to enhance safety across its site and provide an efficient journey for users. With this powerful video security system, the operations team can rely on its technology to provide the extensive coverage they need to perform their duties. Feedback from CBBT has been overwhelmingly positive, in particular around the significant improvement in the coverage area, imagery and ease of use.

“

The coverage achieved using Pelco has allowed us to shorten our response times. When an event occurs, we can pinpoint where to send help, and it arrives sooner.

Ray Wood
DIRECTOR OF MANAGEMENT
INFORMATION SYSTEMS AT CHESAPEAKE BAY
BRIDGE-TUNNEL

[Read case study](#)

CASE STUDY



Streamlining traffic flow and enhancing security for a large airport

With so many passengers coming and going from Memphis Tennessee Airport, it sees a substantial number of vehicles entering and exiting the facility. To streamline traffic and ensure staff could be deployed quickly to a specific parking floor or location to alleviate any problems, the airport deployed Pelco's video security system.

Once the system was deployed, its potential security applications quickly became apparent and have proven valuable in several incidents, including instances of individuals driving through or breaking parking arm gates to avoid paying fees. In these situations, cameras captured license plate information, allowing the drivers to be identified and held responsible for parking fees and the damage they caused.

In another situation, the video system helped the airport as well as the TSA avoid liability and a potential lawsuit when a woman accused TSA of harassing, beating and injuring her daughter, a brain cancer patient from St. Jude Children's Hospital. Cameras showed that the TSA agent had merely restrained the girl after she had swung at and attacked him.

[Read case study](#)



School district adopts smart sensor system to improve student safety

The biggest challenge for Castleberry Independent School District (ISD) before and during the pandemic was vaping in the bathrooms. With the return of students and staff, the administrators were not only looking for a way to curb vaping but also ensure that air quality was as clean as possible to prevent the transmission of viruses.

When administrators were shown the Halo Smart Sensor, they recognized that the device went beyond just vaping and that it could also monitor air quality. Since deploying these smart devices across the school, the school saw a spike in vaping and uncovered an air quality issue that would have never been found in the older buildings.

[Read case study](#)

“

Our decision to select Halo was based on the versatility of the sensor and the positive reviews from other schools. We made the right decision deploying Halo within our school district as it's protecting our school privacy areas and also providing security while protecting individual privacy.

Samuel Cervantez
SAFETY/SECURITY COORDINATOR
AT CASTLEBERRY ISD

Final thoughts on physical security

Physical security is fundamental to your business' success. With the right physical security measures, it need not be expensive or difficult to maintain.

The best way to improve workplace safety and security is to carefully observe exactly what your company needs and to find the right physical security tools, technology and methods for the job.



Additional resources

- ▶ [Commercial security camera industry trends guide](#)
- ▶ [Physical security assessment & checklist](#)
- ▶ [School security systems guide](#)
- ▶ [ONVIF cameras and profiles guide](#)
- ▶ [Security camera cable & wiring guide](#)



Get expert **help** today