kisi

The complete guide to physical security

45 Main Street,
11201 Brooklyn
USA

sales@getkisi.com
getkisi.com

kisi

Table of contents

Introduction

Security is crucial to any office or facility, but understanding how to get started or upgrade to modern security can be challenging.

Even in small spaces, there can be dozens, if not hundreds, of moving parts that can confuse even the most seasoned business professional.

The right resources, tips, and tricks can help you make and implement reliable decisions on protecting your business, people, and assets. Our complete physical security guide aims to do just that.

What is physical security?

Physical security covers the measures companies take to protect people, property, and assets from physical threats like theft, vandalism, or natural disasters. It involves a combination of physical barriers, technology, and personnel to deter, detect, and respond to potential threats.

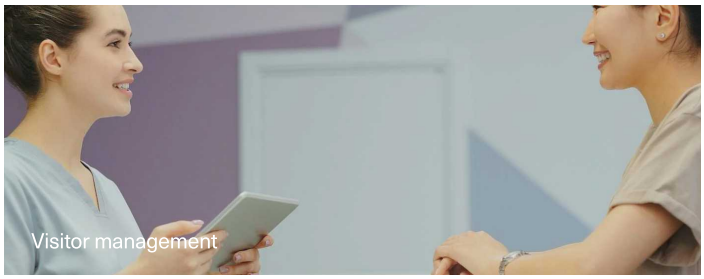
Key elements of a comprehensive physical security system include:

- Access control: Managing entry to buildings or sensitive areas using mobile or physical credentials, like badges in Apple Wallet, keycards, or QR codes, to ensure only authorized people can enter.
- Video surveillance: Monitoring premises with cameras and video analytics to deter and detect malicious activity and provide real-time visibility of potential security threats.
- Intrusion detection: Using alarms, motion detectors, and sensors to detect unauthorized access or suspicious activity that trigger real-time alerts to relevant personnel.
- Visitor management: Tracking and managing visitors, ensuring all guests are checked in and identified.
- Data and analytics: Leveraging data from surveillance, access logs, and sensors to ensure compliance, identify patterns, optimize security protocols, and enhance decision-making.

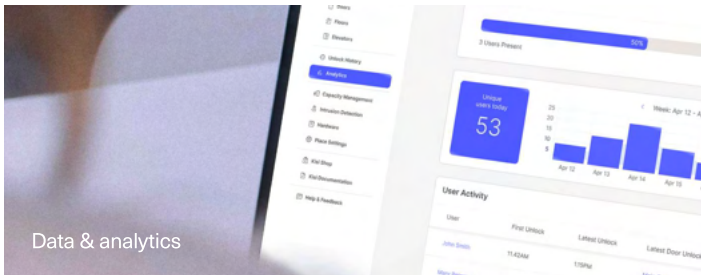
Integrating these physical security elements is crucial for businesses to ensure the safety of sensitive data, equipment, and employees. By combining technology with strategic planning, physical security minimizes risk and strengthens overall safety and security. Modern, cloud-based physical security goes a step further by centralizing all elements and spaces behind a single pane of glass, improving accessibility and user experience and cutting overhead by streamlining operations.


Access control


Video surveillance


Visitor management


Intrusion detection



Data & analytics

Kisi Inc.
sales@getkisi.com
getkisi.com

Physical security threats

Physical security threats are risks that can compromise the safety of your property, people, and assets. Companies lost more than USD$1 trillion in revenue due to physical security incidents in 2022. Recognizing and understanding these threats is essential for choosing the right physical security tech and designing effective security measures for your company.

The most common physical security threats businesses face include:

- Unauthorized access: If individuals gain entry to restricted areas without permission, it can lead to theft, data breaches, or sabotage. Outdated access control can make facilities vulnerable, with 18% of companies experiencing trespassing, 21 malicious damage to company property, and 15% intrusion, according to the 2022 World Security Report.

- Theft and burglary: Bad actors targeting valuable assets such as equipment, inventory, or sensitive data can cause significant financial loss. Cloud-based access control systems with integrated security cameras and alarms are critical in preventing and mitigating these crimes. Integrated, modern physical security systems are becoming a necessity, with 22% of companies experiencing theft of company physical property.

- Vandalism: Damage to property, often motivated by malice or protest. The financial repercussions can amplify if the intruder vandalizes critical infrastructure, leading to a bigger operational shutdown, resulting in revenue losses and a tarnished company image, often resulting in stock price drops. Cloud-based physical security systems that include video surveillance and physical barriers can deter vandals.

- Workplace violence: Threats from disgruntled employees, customers, or external parties pose a serious danger to staff and operations. According to the Bureau of Labor Statistics, there were 57,610 nonfatal cases of workplace violence, 71.6 percent of which resulted in at least one day away from work over the 2021-2022 period. Proactive measures, including automated access control and video surveillance, help prevent and mitigate these risks.

- Natural disasters: Events such as fires, floods, earthquakes, or severe weather can destroy company assets and threaten human life. Around 12% of companies reported revenue losses related to a natural disaster in 2021, with companies with more than 50 employees and higher revenues reporting losses exceeding $100,000. Businesses need emergency preparedness plans, reinforced structures, and disaster recovery strategies. Conducting a thorough risk assessment to implement relevant structural and non-structural mitigation measures is crucial for reducing damage. Effective communication and coordination are vital, and integrating a physical security system with emergency capabilities, including roll call, can facilitate a more effective response and recovery process.

- Tailgating and piggybacking: Social engineering attacks when unauthorized individuals follow or impersonate authorized personnel into restricted areas without proper credentials, bypassing access control measures can create safety, financial, and reputational concerns for an organization, all without anyone realizing that it's happening. Integrating advanced access control and video surveillance solutions can detect tailgating. Timely employee security training can also help mitigate this threat.

Physical security audit

Conducting a comprehensive audit of your organization's physical security measures is essential in identifying vulnerabilities, evaluating the current system, and uncovering improvement possibilities. Doing a yearly assessment ensures that your security systems and protocols effectively safeguard facilities, people, and assets against threats.

Security audits should be extensive and cover a lot of components. Pay special attention to the following key components:

- Environmental components: The building's location and terrain can provide security or reduce the means of attack and unauthorized access. A visible distinction between the building's and public properties, a perimeter buffer zone or stand-off barriers, as well as landscaping and external aesthetics that can serve as hiding places or means of access to other secluded access points, are important to consider.

- Physical barriers and access points: If your property has gates, ensure they are secure and operate properly. All other access points to the property, including doors, turnstile, and windows, are secured and can be locked. Evaluate bollards, reinforced glass, doors, partitions, hinges, and framing.

- Lighting: Check if internal and external lighting is functioning in all required areas and if exterior lights are mounted high. Adequate lighting allows guards, employees, and others to see possible concealment and access places, so it needs to be regularly inspected and maintained. Back-up lighting should be available in the case of a power failure.

- Access control: Inspect if you monitor all external access points using manned positions or technology to ensure employees, occupants, and contractors enter and exit the facility through a secured access point. Door readers are installed at all places you want to limit who has access, and the access control system is extended to elevators for improved floor security. The access control system is reliable and can easily support the constant flow of people during the busiest hours.

- Surveillance and intrusion detection: Video cameras are strategically placed to monitor the entrances, exits, stairwells, and other access points. The footage is constantly monitored, and you have an integrated video management system (VMS) that alerts you of important events. Camera footage of all key access events is reviewed and maintained to allow for investigations. All secured access points are equipped with access readers or sensors that detect forced entry, while all alarms are functioning properly and are tested regularly.

- Physical security operations: There is a person designated to lead all security-related activities who understands both the technology and the legal aspects and has a modern perspective on security to grasp all the risks and potentials. Documented procedures for reviewing the general security program are in place, and regular self-assessment of security practices, procedures, and policies according to risk is conducted. Procedures are in place for a prompt internal investigation of any security-related incidents and security documentation is updated promptly when procedures or equipment are changed or newly implemented. Documented policies are in place and followed for the use, maintenance, protection, and regular inspections of security technology (e.g., locks, lights, access control, and cameras).

Physical security audit

- Access control operations: Documented procedures define access control privileges for different employee groups and visitors, and admins can remotely manage access and unlock doors to all secured locations. New users are quickly onboarded and have access only to the necessary places from day one. Automated door schedules and restrictions are in place, and users who no longer require access have their access permissions promptly revoked. Access points can be audited, and an audit trail is available to trace security-related events back to their source. Your access control software is regularly updated to reduce security risks and cyberattack vulnerability.

- Communication, training, and alerts: A security awareness program is regularly conducted so users can adhere accordingly to effectively communicated security policies and procedures. Employees are comfortable with and understand why they need the various security measures, are encouraged to learn their security obligations, and are familiar with the resources available to help with security concerns. Admins get instant alerts on their mobile phones when violations occur (e.g., when a door is forced or propped open) so they can take immediate action.

- Emergency response readiness: You can identify potential natural disasters, and a plan is in place to respond to each type of disaster, including emergency evacuation procedures, emergency communications protocols, and emergency supplies. You track occupancy to meet everyday and emergency needs and stay compliant. All critical security technology systems are connected to alternate power sources, and smoke and fire detection systems are set up properly and regularly tested. All doors can be locked and unlocked remotely and specific doors can be put on lockdown to contain an attack, intruder, or accident. Tenants and staff are trained for emergency egress with clearly marked exits and evacuation routes. The security system allows for positive identification of who is in the building in case of an emergency.

Tick all the boxes with our downloadable audit checklists

→ Building security checklist
→ Physical security risk assessment for tech companies
→ Physical security audit checklist for manufacturing companies

Physical security best practices

The specific security practices you should implement when creating a solid physical security strategy always depend on the specifics of your premises and the nature of your business. Still, many physical security plans share certain core elements. Working examples of security strategy and countermeasures in physical security have a number of best practices in common:

- Secure the parameter: Establish physical barriers like fences and gates to deter intruders as your first line of defense. Adequate lighting, motion detectors, and signage can also strengthen perimeter security and discourage the average passerby from entering your security perimeter.

- Add video surveillance: Deploy video cameras strategically around entry points, high-traffic areas, and sensitive locations. Ensure that cameras are constantly monitored or connected to your access control system so you can get the most critical real-time alerts and prevent tailgating. Ensure footage is stored securely for future review and audits.

- Track and manage visitors: Implement a modern visitor management system that helps you manage and track all visitors entering the premises. Visitors should be enabled to check in smoothly and be provided with temporary credentials that should last for the duration of the stay and which they can only use to gain access to the necessary areas.

- Enable intrusion detections: Install alarms, motion sensors, and door/window sensors to detect unauthorized entry. Ensure these systems are integrated with your access control system so admins can be notified to respond to and mitigate potential breaches.

- Conduct security audits and maintain equipment: Audit your security systems at least once a year to identify potential vulnerabilities and areas for improvement. Regularly inspect and maintain all security equipment, including locks, cameras, alarms, and access control systems, to prevent failures and ensure optimal performance. Cloud-based systems usually provide automated over-the-air (OTA) updates, but if you are using legacy access control, make sure to update the software as well and introduce new functionalities as needed.

- Train employees on security protocols: Ensure all staff are trained on physical security policies, including how the access control system works, how to recognize and report suspicious activity, handle visitors or tailgating, and respond to emergencies. Regular training reduces human error, which is a common vulnerability.

- Prepare for emergencies: Have clear emergency procedures in place for incidents such as natural disasters, like fires or floods, theft, or workplace violence. Ensure admins get notified of potential emergencies and can quickly and remotely lock down certain doors or initiate lockdown on all secured doors to contain or prevent the emergency. Conduct regular drills and ensure all staff are familiar with evacuation routes, roll call practices, and emergency contacts.

- Leverage data, reporting, and analytics: Use security analytics tools to monitor access logs and video footage to identify trends, help anticipate threats, and optimize security measures. If possible, schedule regular reports to ensure compliance and track events and users, as well as place analytics and access permissions.

Access control

If you carry an access card, ID badge, or keyfob then you already use an access control system. But how does it really work? Laymen initially believe it's just a card reader on the wall. Once you get deeper into access control, you realize a few behind-the-scenes parts make unlocking possible. Let's explore how access control systems work, their benefits, how they fit into the security puzzle, and what's the best use case for you.

What is physical access control?

An access control system allows you to manage, monitor, and maintain who can unlock certain doors and at what time they can access them. The simplest access control “system” is a standard deadbolt with a brass key. The basic modern access control hardware consists of an access controller, reader, and credentials.

Access control systems are not restricted to doors. You can manage access to different objects, including the most popular: Windows, elevators, gates, lockers, and printers. The standard form of workplace access control is moving from on-premise solutions to the cloud, while the preferred access method transitions from an access badge to a mobile credential.

The increasing security threats make access control a necessity. The interoperability of modern access systems makes it possible for every business, even ones located in multi-tenant buildings, to take control of their access management.

Benefits of an access control system

The purpose of access control is to provide quick, convenient access control for authorized persons while, at the same time, restrict access for unauthorized people. Besides the evident security reasons, there are additional benefits to implementing an access control system:

- Enhanced security: Besides preventing unauthorized people from entering your building or specific areas, modern access systems enable you to manage visitors and set access groups and schedules for different user groups like full-time employees, contractors, and vendors.

- Monetization with data insights: Modern automated access control can drive revenue for your business by reducing operational overhead or increasing operation hours without hiring extra staff. The access control data insights can help you optimize space utilization, especially when enforcing hybrid work models.

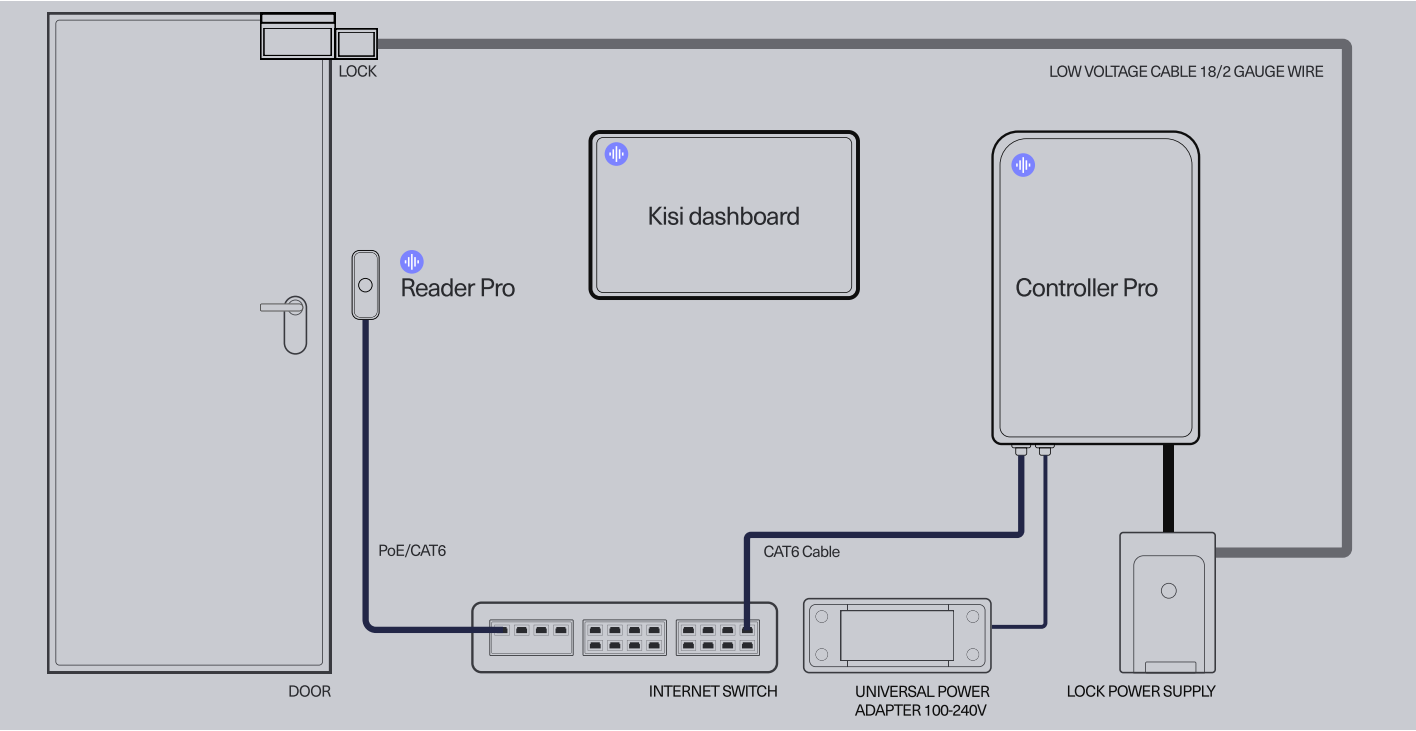
- Compliance: Having a certified access control system like Kisi increases your credibility, makes you safer and better protected against malware and hackers, and ultimately leads to increased revenue. Access control is even more important for regulated industries that need to be compliant, such as healthcare and financial institutions, and most tech companies that need to maintain SOC2 cybersecurity standards.
- Streamlined operations: Integrating with your directories to automate user provisioning and de-provisioning means that on- and off-boarding processes are on autopilot, reducing maintenance and manual tasks for your admins and also decreasing the chances of human error. By automating access control, you can reduce operational costs and save around $100 per person in the first year.

- Visitor management: Access control also streamlines visitor management procedures by ensuring no visitor has access to your facility without being previously authorized by an admin who can allow them to access the areas they need during the time of their stay.

- IP and data protection: Businesses dealing with privileged data and intellectual property, such as software developers, law firms, entrepreneurs, and pharmaceutical companies, need to control and log not only who comes into their facilities but also which areas these individuals are allowed to access and when.

- User experience: Leveraging technology that offers a smooth access experience and higher control on the admin side can support the return to the office and promote collaboration and productivity opportunities. Implementing mobile access means empowering users to unlock any doors they have access to using their phones, taking convenience to another level.

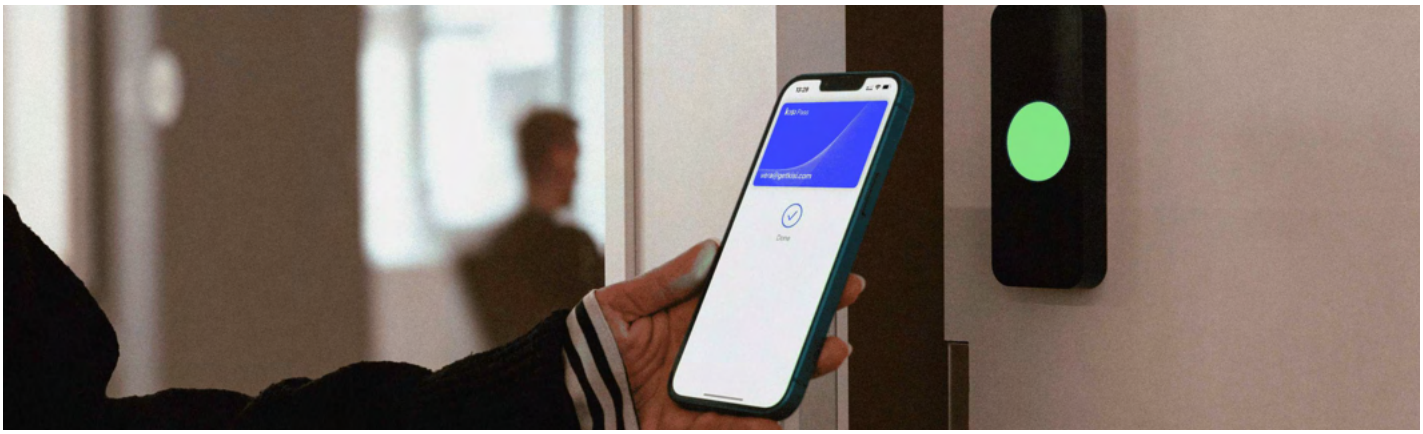
Access control components



Access control systems vary widely in type and complexity. Still, most access control systems consist of similar basic components that can be divided into three groups:

1. User-facing
2. Admin-facing
3. Infrastructure components.

User-facing components

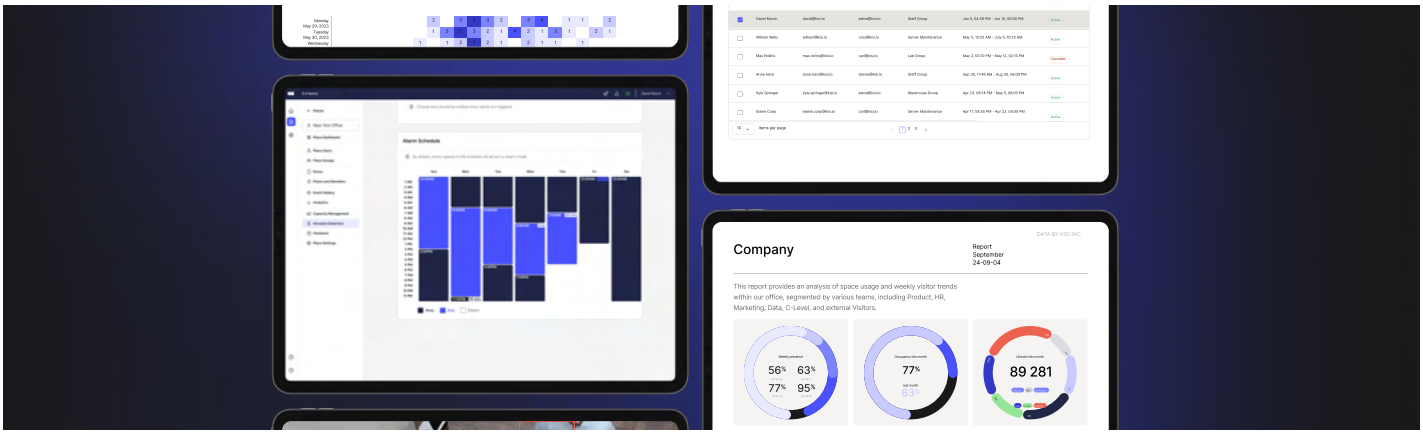


Essential for managing and securing access to restricted areas, user-facing access control components are the ones users perceive and interact with, making them vital for seamless user experience and convenience. Users usually come across the following components:

- Access reader: The device usually mounted near doors or other entry points that verifies users' credentials, using technologies like RFID or NFC. Advanced readers, like the Kisi Reader Pro, support multi-factor authentication, integrate with other security systems, and allow different mobile access methods, enabling a convenient and seamless user experience. Besides enhancing security, some readers allow real-time connectivity and auditing capabilities, offering additional functionalities like capacity management and intrusion detection.

- Credentials: Keycards, ID badges, fobs, and smartphone apps, collectively known as access credentials, hold the user's data that the reader uses to verify if the door should be unlocked. Proximity cards, as well as phones, typically need to be held 2–6 inches from the reader. Credentials offer an advantage over traditional keys by being personalized, allowing access events to be traced back to specific individuals. Check out our access control methods assessment to explore the various credential options available, including employee badges in Apple Wallet and QR codes, and discover which one would work best for you.

Admin-facing components



The admin-facing side of an access control system is the management dashboard. Authorized users, such as office administrators or IT managers, use it to set access permissions and schedules, determining who can access specific areas and under what conditions.

Modern businesses often use cloud-based dashboards for remote management and advanced features. Advanced systems, like Kisi, allow automation of tasks like issuing credentials by integrating with employee directories through APIs or services like Google Apps, Microsoft Entra ID, or Okta.

Infrastructure components

Most users are less familiar with the infrastructure components, like access panels, locks, and cables, given they're closely connected to the building infrastructure. While most infrastructure components are necessary for the access system to work, some can serve to help companies migrate to the cloud with ease:

- Electronic locks: Typically wired to receive power, electronic locks provide keyless entry. There are two types: Fail-safe locks, which lock when powered and unlock during power loss (suitable for entry doors to meet fire and safety codes), and fail-secure locks, which remain locked without power (ideal for IT rooms needing constant security).

- Controller: The central hub for managing access to secured areas, typically hidden in the IT or server room. When a valid credential is presented to a door reader, the controller receives the request to unlock a specific relay connected to the specific door wire.

- Server: Modern access control systems are cloud-based, eliminating the need for a local server to enhance security, reduce costs, and simplify the user experience. In contrast, legacy systems require on-site management via a dedicated server, making remote administration difficult and complicating management across multiple locations and hybrid setups.

- Low-voltage cables: A critical part of access control, cables can be one of the biggest expenses when purchasing or upgrading an access control system. Failing to plan for cables can lead to costly and disruptive retrofitting, requiring additional labor to lay cables or drill into walls later on.

- Wiegand board: Added to the Kisi Controller Pro 2, it's ideal for upgrading an existing access control system to the cloud. It allows businesses to reuse legacy hardware while enabling necessary functionalities like remote management and automated workflows. Installation is straightforward, with no downtime or need for wiring changes.

- Two-wire switch and adapter: Upgrade to the Kisi access control platform at minimal cost while retaining your existing wiring. These accessories eliminate the need for new CAT6 cables, reducing installation expenses and enabling easy and secure scaling by adding new doors and users with just a few clicks.

Enhance your security with seamless access control

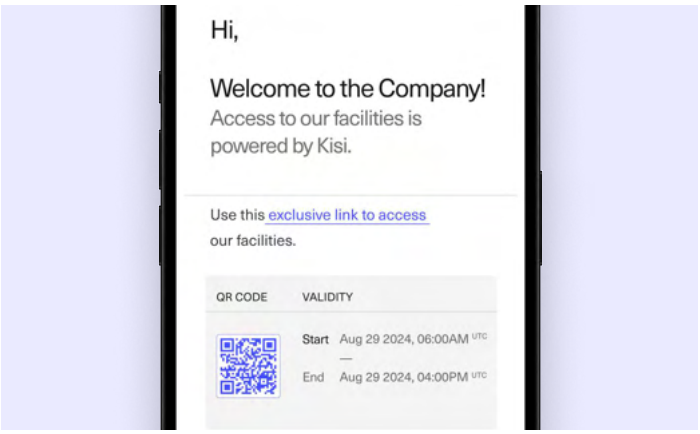
Ensure the safety and efficiency of your space with Kisi's award-winning hardware and access control solution, designed to deliver unparalleled flexibility, reliability, and ease of use. → Access control system → Access control guide

Visitor management

Whether you're interviewing new hires, hosting an event or potential clients, or expecting hired contractors, visitors are unavoidable in any business setting. While trying to create a welcoming experience for visitors, businesses need to consider valuable resources, private information, and sensitive data that can fall into the wrong hands. Modern visitor management systems enable you to impress visitors while ensuring compliance and security.

Understanding visitor management

Unlike the old-fashioned method of logging visitors by hand, modern visitor management systems enable you to assign temporary visitor credentials and keep track of who is in your space and where they are at all times. Encoded in each credential, usually a badge, link, or QR code, is a unique identifying number for the credential holder. Each ID number has a designated level of access, allowing the visitor to access certain doors during a specific period.



A certain feeling of trust is inspired in visitors when they have access to the needed space even before they are greeted by the receptionist or they are able to self-check in if the process is automated. As a first impression, this action makes your organization appear modern, welcoming, and diligent. On your end, this action ensures that everyone who enters your space has entered identifying information into your system, meaning you have logs for compliance and potential incident mitigation.

The value of electronic visitor management is not only about giving that special guest treatment. Among other perks, it amplifies the worth of your current business, creating an extra real estate opportunity. Office buildings with a proper visitor management system often sell or rent for higher rates than comparable buildings without it.

Benefits of visitor management

Vital for modern organizations, streamlined visitor management enhances security and reduces operational overhead. Whether for office buildings, industrial facilities, or educational institutions, automated visitor systems offer the following benefits:

- Enhanced security: Just the fact that you have a visitor management system can scare off potential bad actors. For instance, if someone is doing a hostile reconnaissance and notices that their visit is only recorded on paper, they might be more likely to attempt a burglary. You also reduce theft by preventing visitors from unauthorized areas and times outside their visit. Combining access control systems, visitor management, and video surveillance should keep any wrongdoers away. In case someone with malicious intent has managed to get access, detailed records of visitor check-ins and -outs can track who is on-site at any given time, ensuring accountability and resolution.

- Reduced operational overhead: You can automate, streamline visitor processes, and replace manual tasks, such as guest registration, with self-check-in and temporary access credentials, minimizing the need for front desk staff involvement. Digital records management and visitor management software eliminate paper logs, making it easier to store, search, and manage visitor data in the cloud, while automated notifications alert hosts when their guests arrive, removing the need for manual communication. Integrate with your access control system to issue temporary credentials, like access links and QR codes, or print visitor badges to improve workplace efficiency.

- Compliance: Automated tracking and managing visitor data ensures accurate and up-to-date records that meet regulatory requirements. Eliminate the need for manual record-keeping and reduce the risk of human error with digital logs of every visitor's entry and exit. The ability to generate and export detailed, time-stamped reports on visitor activity simplifies audits and ensures organizations remain compliant, especially in highly regulated industries like healthcare or finance.

- Professional impression: Impress visitors and enhance professionalism by providing a seamless and modern experience. Integrate access control to enable guests to unlock the front door with their phone without even needing to ring the doorbell. Greet them with sleek, intuitive self-check-in processes, eliminating the need for manually filing sheets. Reduce wait times with automated host notifications to instantly inform them of their visitor's arrival. Customize and brand visitor badges and emails to reflect corporate identity, reinforcing the company's image and creating a consistent, high-quality experience from the door.

- Analytics and reporting: Make informed, strategic choices with data-based decisions based on valuable insights and analytics on visitor activity. Optimize resources, staffing, and security measures based on real-time insights and detailed reports on visitor patterns, like peak hours, frequent visitors, and visitor types. Analyze visitor data to identify trends, such as which departments or employees receive the most guests or which maintenance contractor is most productive, to adjust workflows or allocate resources accordingly. Evaluate and mitigate potential security risks and incidents with detailed reports.

Explore visitor management

Replace outdated paper systems with a seamless digital solution that enhances visitor experience, maintains a secure environment, and ensures compliance with detailed visitor schedules.

→ Visitor management → Visitor management guide

Video surveillance

Playing a critical role in any comprehensive physical security plan, video surveillance serves as both a deterrent to potential threats and a tool for monitoring and protecting assets. Modern surveillance systems no longer consist of a bunch of CCTV camera monitors with recorded footage that someone needs to keep an eye on 24/7. They integrate with advanced technologies like access control, motion detection, facial recognition, and cloud storage to provide real-time monitoring, long-term data retention for ease of incident resolution, and tailgating detection.

Benefits of video surveillance

High-definition cameras, remote management through mobile devices, and intelligent analytics are some of the capabilities advanced video surveillance systems boast. A modern video surveillance system ensures you maintain visibility over critical areas and can respond swiftly to any suspicious activity. Improving security, reducing liabilities, preventing theft, and maintaining compliance are just some of the benefits:

- Real time monitoring: Modern business security camera systems enable premise monitoring in real time and store the footage in the cloud, giving security teams or managers the ability to respond quickly to incidents. Remote management functionalities enable monitoring from mobile devices, providing extra flexibility and timely responses from anywhere. Real-time alerts in case of suspicious activity at entry points are possible by integrating access control and video security.

- Crime deterrence: The presence of visible security cameras is a strong deterrent to theft, vandalism, and other criminal activities. Potential wrongdoers are less likely to target a location where they know their actions are being recorded regardless of its potential external intruders or authorized personnel. International research states that surveillance cameras usually decrease reported crimes in urban environments by 20-25%.

- Evidence: Video footage can provide valuable evidence that you can provide to law enforcement in potential security breaches, accidents, or disputes. According to research, 86% of occupational fraud is due to asset misappropriation – an employee stealing or misusing the employer's resources, with a median loss of $100,000 per case. Having video surveillance can be crucial in resolving legal claims, employee disputes, or insurance matters and protecting your business from false accusations and litigation.

- Detect tailgating: Holding open a door for someone is polite but can pose a serious security risk. A tailgating attack can create safety, financial, and reputational concerns for an organization. By connecting video surveillance with access control, you can detect unauthorized individuals following authorized personnel in your organization, identify potential security breaches, ensure a secure environment, and improve compliance.

- Employee accountability: Workplace surveillance can help ensure employee accountability by monitoring workspaces and sensitive areas. Businesses can track suspicious activities and hold individuals accountable through recorded footage. Keeping a watchful eye on valuable assets, high-traffic areas, and workspaces discourages workplace misconduct, time theft, and non-compliance with company policies, leading to more responsible behavior.

- Compliance: By keeping documented visual records, businesses can easily demonstrate adherence to safety, security, and operational protocols, helping to avoid fines, penalties, or legal issues related to non-compliance. The footage archive can additionally provide evidence for audits or investigations if necessary.

Types of security cameras

Security cameras, in some form or another, have been around for decades, ranging from clunky old CCTV systems with pixelated monitors to modern, AI-enhanced HD solutions. Nowadays, they come in many shapes and sizes, with some solutions more adapted to typical offices and some to large facilities or multi-tenant buildings. This section will cover the most common and popular security camera types.

Dome cameras

Named for the shape of their housing, dome cameras are a popular choice for indoor and outdoor security due to their discreet design and versatility. The dome design protects the lens from environmental factors and vandalism while making it difficult for intruders to tell which direction the camera is pointing. Equipped with advanced features like night vision, weatherproof casings, and high-resolution video, modern dome cameras are ideal for monitoring large areas such as retail spaces, offices, or warehouses and are usually the go-to solution for businesses looking to enhance security without compromising aesthetics.

Bullet cameras

Commonly used for long-range monitoring in outdoor environments, the cylindrical design allows for highly focused surveillance, making bullet cameras perfect for securing entrances, parking lots, and perimeter fences. Often weatherproof, their sturdy housings can withstand extreme temperatures and harsh conditions. Modern bullet cameras boast ultra-HD video, wide dynamic range (WDR) for handling varying light conditions, and infrared (IR) capabilities for superior nighttime visibility. When connected to an advanced VMS system, these cameras can be used for license plate recognition and people counting.

Pan-tilt-zoom (PTZ) cameras

Suitable for large spaces like stadiums, airports, or industrial facilities, the camera's ability to pan, tilt, and zoom gives users precise control with wide coverage and flexibility. Operators can adjust the camera's view in real-time or program it to move automatically between preset positions, ensuring maximum area coverage with minimal blind spots. Modern PTZ cameras incorporate AI for automated person or vehicle tracking across multiple zones. The automation capabilities, high-resolution imaging, and powerful optical zoom make PTZ cameras ideal for businesses with high-security demands, critical infrastructure, or high-traffic areas requiring constant surveillance.

Fisheye cameras

With an innovative lens curvature that enables a 360-degree panoramic view, businesses can monitor large areas with a single fisheye camera. The unique lens design minimizes blind spots, capturing footage from all directions, making fisheye cameras the go-to choice for open spaces like lobbies, retail stores, or warehouses. Suitable for most businesses looking to cover large areas with minimal hardware, fisheye cameras are a cost-effective and efficient surveillance option. Modern fisheye cameras boast de-warping technology, which corrects the distorted image typical of fisheye lenses.

C-mount cameras

Known for their adaptability, C-mount cameras feature detachable lenses that can be switched for the desired focal length and customized for different security needs, like monitoring vast outdoor spaces or small indoor areas. C-mount cameras are usually used in industrial settings or large commercial buildings where specific areas require high-detail monitoring. Modern C-Mount cameras include 4K imaging, weather-resistant features, and powerful zoom options, increasing their versatility. Integrated with modern security systems, C-Mount cameras can provide detailed close-ups and broad overviews, ensuring comprehensive surveillance coverage.

Infrared (IR) cameras

Using infrared LEDs, IR cameras can capture sharp, black-and-white images at night, making them ideal for businesses needing round-the-clock surveillance and nighttime security, like warehouses, parking lots, or construction sites. Designed to automatically switch between color during the day and infrared at night, these cameras ensure reliable surveillance in varying light conditions. Many newer models incorporate smart IR technology, which adjusts the intensity of the infrared light based on the object's distance, preventing overexposure and ensuring accurate image capture.

Types of security cameras

Internet protocol (IP) cameras

IP cameras use digital video technology to transmit data over a network, deliver high-quality video, and are easily integrated with other systems, such as access control or alarm systems, making them a gold standard in modern surveillance systems. Thanks to video compression and bandwidth optimization advancements, IP cameras now provide ultra-clear footage with minimal latency. As part of a video surveillance system, modern models can provide intelligent analytics, including people counting, object detection, and automated alerts, helping businesses improve security and reduce operational overhead. Due to their scalability, they are suitable for all businesses, from small offices to multi-site enterprises.

Thermal cameras

Detecting heat signatures instead of visible light, thermal cameras are ideal for environments where visibility is compromised, like during nighttime, fog, or smoke-filled conditions. Widely used in critical infrastructure, such as power plants or airports, these cameras can detect unusual temperature fluctuations and signal equipment failures or fire risks. Thermal cameras that integrate with other security systems have become more accessible to commercial businesses and are particularly valuable in areas where low visibility makes conventional cameras ineffective in identifying potential threats.

Wireless cameras

Offering easy installation and flexibility, wireless cameras rely on Wi-Fi or other wireless protocols to transmit footage to a central storage system or cloud platform, enabling remote monitoring via smartphones or computers. Especially useful for temporary setups, such as events or pop-up locations, or businesses looking to avoid intrusive installations with complex wiring. Modern wireless cameras can have long-lasting battery life, solar power options, and advanced encryption for secure data transmission. They can also offer high-definition video, two-way audio, and AI-based analytics, such as facial recognition or motion alerts.

Covert cameras

Covert cameras provide businesses with an effective way to discreetly monitor sensitive areas without drawing attention to surveillance efforts. These hidden cameras are especially useful in environments like offices, retail spaces, or warehouses where visible cameras might alter behavior or lead to tampering. By capturing unfiltered actions, covert cameras play a crucial role in identifying internal theft, unauthorized access, or inappropriate behavior without alerting those being watched. This element of surprise makes covert cameras valuable for gathering critical evidence in security breaches or compliance audits, particularly in industries where high-value goods or sensitive data are at risk.

Dummy cameras

Dummy cameras, while appearing to offer a cost-effective solution, often fall short in business settings. Although they may deter casual theft or vandalism, experienced criminals can easily identify them as non-functional, potentially encouraging further attempts once they realize there is no real surveillance in place. In compliance-heavy industries, such as finance or healthcare, relying on dummy cameras can lead to regulatory penalties, as these sectors require actual, functional security systems. While dummy cameras might offer superficial appeal due to their low cost and ease of installation, businesses are better off investing in real surveillance systems to ensure both security and regulatory compliance.

Modern security camera features

Modern cameras have advanced features that offer businesses enhanced visibility, real-time alerts, and powerful data-driven insights. Regardless of how large and complex the space you're securing is, the right camera system can deter crime, improve safety, and provide analytics to help with operational decision-making, incident prevention, and workflow optimization. Let's go through some of the key features to consider when selecting your next security camera:

Wireless IP connectivity

Most modern security cameras use IP connectivity technology, meaning information is transmitted as if the camera were a computer, measured in megapixels, and transmitted over the network. Connecting to your network without extensive wiring, wireless IP cameras are flexible, easy-to-install solutions for expanding businesses or those looking to avoid the high costs of traditional cabling. Managers or security personnel can monitor facilities remotely by accessing security footage in real-time. The wireless IP connectivity enables integration with existing IT infrastructures to build a scalable and future-proof security system that can adapt to changing needs or physical layouts.

Video compression

High-resolution video makes efficient storage essential. Modern video compression technologies like H.264 and H.265 allow businesses to store large amounts of footage without overwhelming storage capacity. By significantly reducing the file size of recorded footage, these compression standards allow businesses with long retention periods or those using cloud storage solutions to maintain high-quality video recordings while minimizing storage costs and bandwidth usage.

Alarm I/O

Alarm I/O is a powerful feature that enhances business security by integrating cameras with other security components like alarms, motion sensors, or access control. This way, alarms can be automatically triggered or even doors locked when a camera detects suspicious activity, like unauthorized access or movement during off hours. This level of automation not only strengthens security protocols but also reduces the need for manual intervention, allowing businesses to respond swiftly to potential incidents while reducing the risk of human error.

Durability and weather resistance

Durability is crucial for businesses with outdoor security cameras, especially in harsh weather conditions. Modern cameras built with robust, weatherproof designs, often rated IP65 or higher, are great choices since they continue to operate in rain, snow, or extreme temperatures. If you're concerned about environmental and human threats, vandal-resistant housing should withstand tampering or deliberate damage. Investing in durable, long-lasting equipment enhances security while reducing maintenance and replacement costs.

Focal type

Your choice of focal type will directly affect the field of view of your camera. Varifocal and motorized cameras offer bigger flexibility by allowing operators to zoom in and out and focus on specific areas or objects without losing image clarity. This versatility is ideal for environments where monitoring needs might shift, such as warehouses, retail stores, or parking lots. Choosing the right focal type can significantly enhance the efficiency of your security coverage, ensuring that no critical detail goes unnoticed, whether it's across a large open space, at the entrance, or a narrow corridor.

Tailgating detection

Modern cameras that integrate with VMS or access control systems to enable tailgating detection can identify when multiple people enter a door on a single person's credential and trigger alerts so operators can take immediate action. This feature is essential in preventing unauthorized access to the building, office, or sensitive areas like data centers or labs. With tailgating detection, businesses can enhance access control, maintain compliance, and strengthen their security without constant human monitoring.

High resolution

The leap from standard to HD and 4K resolution in security cameras gives businesses a new level of visual clarity crucial for identifying details like faces, license plates, or even subtle movements. These high-resolution cameras ensure every pixel counts to deliver clear footage that can be the needed evidence in an investigation. The enhanced clarity also means you can zoom in on footage without losing quality, ensuring that even distant or obscured events are captured in detail.

Modern security camera features

Cloud-based

Cloud-based security solutions enable remote access for more accessible, effective, and reliable business security. No longer tied to physical storage systems, companies can store vast amounts of video footage in the cloud, enabling scalability and remote management of live or recorded footage. This streamlines security operations while ensuring rapid responses to potential incidents by allowing operators to monitor multiple locations in real-time, on-site or off-premise.

AI and analytics

AI and video analytics transform cameras from passive recording devices into proactive security tools. Cameras with AI can recognize and alert operators about unusual behavior, such as loitering, trespassing, or crowd formation, so they can prevent these events from escalating into actual security threats. Modern video analytics can distinguish between real threats and false alarms, ensuring security teams focus on what matters most.

Alerts and motion detection

Motion detection technology enables cameras only to record when movement is detected, saving storage space and helping focus on significant events. Combined with real-time alerts that can be received directly on their mobile devices, operators can respond immediately to security breaches or unusual activities. By automating the monitoring process, motion detection reduces the need for constant supervision, making security operations more efficient and responsive, especially useful for after-hours monitoring or high-security areas.

Night vision

Night vision and low-light performance are crucial for facilities that need 24/7 security, like businesses vulnerable to after-hours theft or vandalism. Advanced infrared technology ensures that cameras can capture clear images even in complete darkness, offering uninterrupted surveillance for areas like parking lots, warehouses, or perimeter fences. With improved low-light capabilities, businesses can avoid security blind spots and ensure round-the-cloud surveillance, regardless of lighting conditions.

Explore video surveillance

Elevate your facility's security with Kisi's comprehensive video surveillance system that boasts seamless video event history and advanced tailgating detection.

→ Video surveillance → Video surveillance guide

Intrusion detection

A critical component of any comprehensive physical security strategy, intrusion detection serves as the first line of defense against unauthorized access, breaches, and potential threats. If intrusion detection once meant sounding an alarm when an intrusion occurs, modern systems provide real-time alerts, video verification, and automation capabilities. As business security threats are growing and becoming more sophisticated, implementing an effective intrusion detection system is necessary to reduce the risk of theft, vandalism, and other security breaches.

What is an intrusion detection system?

An intrusion detection system (IDS) is a security solution designed to monitor and detect unauthorized access or unusual activity in a physical environment. An IDS is an early warning system that alerts security personnel to potential breaches or attempts to enter restricted areas so they can react to and proactively prevent potential incidents. These systems use a combination of sensors, detectors, and other technologies to track movements, identify intrusions, and trigger alarms when necessary.

There are several types of intrusion detection systems, each tailored to different environments and needs. For instance, perimeter intrusion detection systems (PIDS) are commonly used outdoors to monitor fences, gates, and other boundaries. These systems often use sensors such as infrared, microwave, or vibration detection to alert security teams of any attempts to breach the perimeter. Inside a facility, interior intrusion detection systems monitor doors, windows, and other entry points using motion sensors, glass break detectors, and pressure sensors. Modern, cloud-based solutions integrate with other security measures like access control, surveillance cameras, and alarm systems to provide comprehensive protection.

Intrusion detection components

Built to address a wide range of security challenges, from monitoring perimeter boundaries to protecting high-security areas, the right intrusion detection components provide full coverage and can integrate with other security systems, like video surveillance and access control. For a simpler understanding, we'll divide the components into sensors, alarms, and infrastructure and management.

Sensors

Sensors are crucial in detecting unauthorized access and triggering alerts, providing the first line of defense by identifying intrusions at critical points, such as doors, windows, and perimeters. There is an array of sensors to choose from that can be integrated with alarms, cameras, and access control systems for a comprehensive security solution. Choosing the right sensors for an intrusion detection system is vital, as each sensor type serves a different purpose.

- Perimeter sensors: Designed to monitor the boundaries of a property and detect any unauthorized attempts to breach the perimeter, perimeter sensors often utilize technologies like infrared, microwave, or even seismic detection to sense disturbances around fences, gates, or walls. Some modern perimeter sensors include real-time monitoring and integrate with AI-powered systems that can differentiate between real threats and harmless movements, such as animals, to minimize false alarms.

- Motion sensors: One of the most popular and versatile sensors for interior security, motion sensors detect movement in secured areas and alert the system. These devices commonly use passive infrared (PIR) or microwave technology to track changes in heat or movement. Modern motion detectors boast sensitivity adjustments to only react to human movement. They can be integrated with security cameras and access control systems to immediately record video upon detecting motion and alert the admin, who can check out the footage and mitigate the potential breach.

- Glass break sensors: Specialized sensors that listen for the specific sound frequency or vibration caused by breaking glass, used for protecting windows and glass doors, which are often vulnerable points in buildings. Modern glass break sensors can distinguish between different types of sounds, ensuring that loud noises like thunder or car alarms don't trigger false alerts.

- Door and window sensor: Typically using magnetic or contact-based technology, these sensors trigger alerts when a door or window is opened without authorization. Besides wired, there are wireless options suitable for easier installation and greater flexibility in placement, but they can be more challenging to maintain due to battery changes. Modern companies often integrate door and window sensors with access control systems to automatically log each event and get insightful data analytics on who enters and exits secured areas.

- Pressure mats: Underutilized yet highly effective security measure, pressure mats are placed beneath floors or carpets, detecting when someone steps onto them. Modern pressure mats can be discreetly placed for covert monitoring and are equipped with adjustable sensitivity settings to reduce false alarms. As part of an integrated security system, pressure mats are handy for securing restricted zones where visual monitoring may be limited.

- Infrared beam sensors: Typically used for monitoring long stretches of space, such as hallways, entryways, or outdoor perimeters, infrared beam sensors project invisible light across the space, triggering an alert when the beam is interrupted. Similar to motion sensors, they can be paired with other sensors and systems, like video surveillance and access control for enhanced security.

- Environmental sensors: While primarily used for detecting intrusions, modern security systems often include environmental sensors that monitor for hazards like smoke, heat, or water leaks. Increasingly integrated into security systems, these sensors are critical for ensuring the safety of occupants, providing businesses with a unified platform for managing both security and building maintenance. They can trigger automatic responses, like sounding an alarm during a fire.

Alarms

Serving as the immediate response mechanism when a breach or environmental anomaly is detected, alarms are designed to notify relevant personnel and sometimes potential intruders that their actions have been detected. Modern intrusion alarm systems are far more advanced than the traditional loud siren. Modern alarms can connect to monitoring services, access control, and video surveillance systems to send real-time notifications with video footage and even trigger automated lockdown procedures.

Having a reliable and comprehensive alarm system is essential to ensuring quick responses to security threats. Let's explore some of the key alarm types and how they enhance modern security systems:

- Audible alarms: Probably the most well-known form of intrusion detection, audible alarms emit loud noises when triggered to alert those nearby and deter intruders. Modern audible alarms can also communicate with security systems to trigger additional actions like locking doors or activating security cameras. Some offer customizable alarm tones and smart speakers that can differentiate between different alarm types, allowing operators to tailor the sound to different levels of urgency or areas within the premises. Others can communicate verbally, announcing specific security breaches to direct staff responses.

- Silent alarms: Designed to notify security personnel or law enforcement without alerting the intruder that their actions have been detected, silent alarms are often used in high-security areas where discretion is key, such as in banks or sensitive government facilities. You can connect silent alarms with modern security systems to automatically send alerts to mobile devices, control centers, or offsite monitoring services and trigger automated responses, like locking down specific doors or activating security cameras.

- Vibration alarms: Detecting movement or vibrations caused by tampering, vibration alarms are an effective option for protecting safes, windows, or doors. Modern vibration alarms can distinguish between everyday vibrations, like heavy foot traffic and actual break-in attempts, reduce false alarms, and provide a more accurate detection profile.

- Panic alarms: Often installed in public-facing areas like reception desks or within secure zones where immediate threats need quick responses, panic and duress alarms enable users to trigger an alarm manually in case of an emergency. Modern panic alarms are often wireless, allowing for discreet installation and easy integration with mobile devices.

Infrastructure and management

Intrusion detection systems rely on a robust infrastructure that enables the seamless operation of the various sensors and alarms. Effective infrastructure supports real-time data transmission, reliable power supplies, and secure communication across all devices. Management tools provide the necessary interface for overseeing, controlling, and maintaining the system.

Here are some of the key intrusion detection infrastructure and management components:

- Access control panel: As the central hub for managing and controlling access to secured areas, access panels or controllers are crucial in an intrusion detection system to coordinate data from sensors, alarms, and access points, deciding when to trigger alarms, notify authorities, or even put places in lockdown. Modern access controllers are cloud-based, enabling remote management, multi-layer authentication, anomaly detection, and seamless integration with other security systems, allowing for a more proactive and responsive approach to intrusion detection.

- Alarm panels: The brains behind the alarm system, alarm panels are responsible for receiving signals from intrusion sensors and triggering the appropriate response, such as activating alarms or notifying authorities. These panels manage the flow of information from various components, deciding when to raise an alarm based on the type of threat detected. Modern alarm panels can be integrated with access control, video surveillance, and other security systems to provide a more comprehensive solution.

- Power supply systems: An uninterrupted power supply ensures that all intrusion detection and security components continue to function even during power outages. Modern power backup systems, like uninterruptible power supplies (UPS) and battery backup solutions, have become smarter, capable of alerting management when power levels are low or switching automatically to secondary power sources. Some businesses adopt renewable energy integrations, such as solar-powered backup systems, to enhance reliability while lowering operational costs.

- Cabling: Essential in connecting all components, high-quality cabling ensures fast and reliable data transmission across the system, allowing for instant alerts and responses when an intrusion is detected. Poor or outdated cabling can result in delayed responses or false alarms, compromising security. Modern systems often use fiber-optic cables for their durability, speed, and resistance to electromagnetic interference. Structured cabling allows for easier maintenance, scalability, and future upgrades as businesses grow or technology advances. In environments where physical cables are difficult to install, wireless alternatives are usually available.

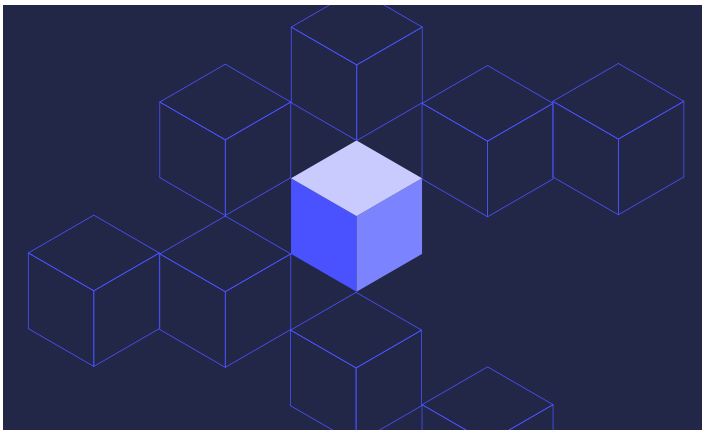
- System monitoring dashboards: Management and monitoring dashboards provide security personnel with real-time insights into the status of all intrusion detection components. Modern cloud-based monitoring dashboards can be accessed remotely and offer intuitive user interfaces, allowing for quick incident analysis, automated reporting, and predictive maintenance alerts. Some systems integrate with AI and machine learning algorithms to provide more accurate threat detection and reduce false alarms, making it easier for businesses to manage complex security environments efficiently.

Explore intrusion detection

Safeguard your premises with real-time alerts and comprehensive coverage for all access points. Gain a holistic view of all security events and activities, enabling quicker identification and response to potential threats.

→ Intrusion detection → Intrusion detection guide

Creating a security plan



Having explored the most important physical security aspects, it's time to move on to creating the security plan. Take a proactive stance toward security, and design a plan that doesn't just respond to existing threats but anticipates and mitigates future risks.

Let's explore the main components of a robust security plan and highlight the essentials to ensuring a resilient and adaptive approach:

1. Applicability: As a first step, define the scope of the security plan, ensuring that each policy and protocol is relevant to specific areas, assets, or personnel. Establishing clear applicability helps streamline the deployment of security measures across departments and locations, ensuring tailored strategies that address each area's unique requirements, like access control and visitor management. For a cohesive yet adaptive approach, layered applicability is advised, where specific departments or high-risk zones are addressed with specialized protocols that complement the broader organizational standards.

2. Risk assessment: Identifying and analyzing potential vulnerabilities across physical and digital areas is essential in resource allocation and minimizing the risk of future incidents. Conduct a thorough review of the premises, identify critical assets, and try to anticipate possible threats. Consider the floor layout, locations, and security of restricted as well as sensitive areas, emergency standby equipment, existing policies, procedures, guidelines, training, and finally, the knowledge of individuals on-site. For a proactive and modern approach to identifying potential weak security points, you can use advanced analytics and even AI to predict potential risks and simulate responses.

3. Roles and responsibility: Essential for accountability and quick decision-making during incidents, establishing clear roles and responsibilities defines which individuals or departments are responsible for specific aspects of security, such as training, monitoring, responding, or reporting. For instance, while the CISO can be responsible for the overall physical security and integrity of data on-site, the Human Resource Officer can exercise additional security vetting processes, like pre-employment background or criminal checks, and be responsible for communicating and passing on the employee handbook that includes the site security plan. The well-defined roles prevent overlapping efforts and ensure a streamlined response.

4. Access control strategy: Define who can access specific areas and at what times to set up the appropriate technology and policy to enforce these boundaries. Decide whether to implement a new cloud-based system or upgrade your current one. Modern access systems are interoperable and offer flexible deployment options to enable remote management, automation, and scalability, making it easier to connect with the rest of your security tech, update permissions, and seamlessly manage multiple locations. Consider upgrading your traditional access credentials, like keycards or fobs, to mobile credentials or add mobile access alongside the physical credentials to provide your employees and visitors with the modern and convenient access experience they expect.

Creating a security plan

5. Surveillance and monitoring: Explore the strategic locations where you need to set up cameras and sensors to detect unauthorized access and monitor or record activity. Update outdated surveillance systems to move to the cloud and introduce video analytics and remote management so you can detect unusual patterns in real time, like loitering or forced entry, and security teams can get instant notifications. Enhance visibility and control by integrating with broader security infrastructure to enable real-time responses and automated actions in the case of a breach.
6. Response protocols: Clear and actionable response protocols are essential for handling security incidents swiftly and effectively. Create a response plan that outlines who should be notified, over what platform, what actions to take, and how information should be documented. Consider using a digital incident response platform connected to your security stack to automate parts of the protocol, send alerts, and generate reports. Establish predefined steps to minimize confusion, reduce response time, and ensure each team member knows their role in a crisis.

7. Data management: Control the collection, storage, and disposal of security data, including access logs, surveillance footage, and incident reports. Implement encryption and access control to secure sensitive information to comply with data privacy regulations. Upgrade to a modern system that integrates data management to ensure all records are securely stored and easily retrievable for audits or reviews, supporting transparency and compliance.

8. Analytics: Collect data from access control systems, surveillance, incident records, and other sources and analyze to identify trends, patterns, and potential areas of concern. Advanced security platforms now offer real-time dashboards and custom reports, enabling key metrics monitoring, such as access frequency, system usage, and incident rates, as they occur. Comprehensive analytics reports ensure that security teams are informed about the efficacy of existing measures, facilitating transparent communication with stakeholders and creating a basis for strategic planning. This data-driven approach also helps to proactively address emerging risks, fine-tune security measures, and can support space optimization.

9. Security testing: Validate the effectiveness of the security measures outlined in the plan with regular system audits, simulated breaches, and policy reviews to identify any vulnerabilities. Routinely test protocols to uncover weaknesses before they are exploited, maintaining a proactive stance on security.

10. Continuous improvement and training: The security plan shouldn't be static but evolve as threats, technology, and business needs change. Regular audits, employee training, and drills are essential to keep the security plan relevant and ensure staff members are prepared to prevent and mitigate potential incidents. Additionally, feedback loops from incidents or near-misses provide valuable insights that can help refine protocols. Allow for real-time adjustments and data-driven improvements by utilizing modern platforms to track and analyze security performance.

Managing low- and medium-security buildings

In low- or medium-risk office settings, physical security combines accessibility and convenience with basic deterrent measures to ensure protection without hampering daily operations. These environments generally don't house highly sensitive assets but hold valuable company resources, private information, and employees who deserve a safe and productive workspace.

Deploying a well-rounded, modern, interoperable security system is essential to enable smooth daily functions and support hybrid work if necessary while securing entry points and monitoring the premises.

The security measures should focus on access control, video surveillance, perimeter protection, emergency preparedness, and policy enforcement. Each component strengthens the overall security posture, helping you maintain a secure environment without disrupting daily workflows. Facilitate easy scaling and modification as the office's needs evolve with a cloud-based solution. Here are some of the core components for streamlining the management of low- and medium-security facilities:

- Access control: Implement mobile access control on primary entry doors and sensitive areas. Set relevant restrictions per user and groups and automate access schedules.
- Video surveillance: High-definition cameras covering entry points, exits, and key common areas connected to video software that enables remote viewing and 24/7 recording with a 30-day storage period.
- Perimeter security: Reinforced entry doors, motion-sensor lighting around exterior areas, and automated door locks outside of working hours.
- Intrusion detection: Basic system with door and window sensors and alarms that automatically alert security or local authorities
- Visitor management: Self-check-in for guests, ability to swiftly issue temporary access, and track visitor activity.
- Emergency preparedness: Clearly marked evacuation routes, fire alarms, and designated assembly points. Routine fire drills and emergency response protocols.
- Periodic security audits: Regular checks of all security components, including door locks, surveillance footage quality, and alarm systems.

Implement these measures to ensure a secure but user-friendly environment for low- and medium-risk buildings, balancing protection with convenience. Going with an open platform with adaptable components enables you to upgrade or downsize these functionalities based on your business needs.

Managing high security buildings

High-risk office buildings, such as government facilities, financial institutions, data centers, or research labs, require a rigorous, multi-layered approach to security. Housing sensitive data, high-value assets, and sometimes personnel in critical roles, these facilities are attractive targets for unauthorized access and breaches.

Security systems must offer more than deterrence. They need proactive threat detection, response capabilities, and constant vigilance to safeguard against advanced threats. A well-integrated security infrastructure enables businesses to establish a robust defense system that effectively deters, detects, neutralizes, and mitigates potential threats.

In high-risk settings, each layer of security, from access control to emergency response, plays a critical role in protecting assets. Advanced access control technology, high-resolution surveillance, and on-site personnel form the foundation, while intrusion detection systems, data encryption, and real-time alerting support rapid response to any potential security event.

Regular threat assessments, reporting and auditing capabilities, and staff training enhance readiness and operational continuity. Here are the basic security components recommended for high-security facilities:

- Advanced access control: Multi-factor authentication systems, including a mix of credentials, like mobile, physical, or biometrics. Automated provisioning, dedicated secure areas with dual-factor entry protocols, and audit trails.
- Comprehensive surveillance: 360-degree high-definition cameras with night vision, infrared capabilities, and automated analytics, like tailgating, motion detection, and facial recognition. Continuous 90-day video storage and tamper-proof systems for critical zones.
- On-site security personnel: Certified security guards stationed at main entrances and sensitive access points, conducting bag checks and frequent patrols. Real-time communication devices for rapid response.
- Intrusion detection systems: Enhanced motion detectors, door and window sensors with tamper protection, pressure mats for sensitive zones, glass-break sensors, and alarms directly linked to security systems to alert relevant personnel and law enforcement.
- Perimeter protection: Anti-climb fences, bollards, automated vehicle gates, security cameras on all building access points, and perimeter lighting to deter unauthorized access.
- Data encryption and cybersecurity: End-to-end encryption of surveillance footage with real-time cyber threat detection and firewall protections for remote monitoring systems.
- Emergency response system: Automated alerts for emergencies with direct lines to law enforcement or fire departments, secure exit points, fire suppression systems in high-risk areas, designated safe rooms, and rehearsed evacuation protocols.
- Regular security drills and threat assessments: Monthly drills for staff and security personnel covering evacuation, lockdown, and emergency response. Quarterly threat assessments to analyze potential vulnerabilities and update security measures.

A comprehensive, multi-layered security plan is essential for high-risk facilities, where protecting assets, data, and personnel is a top priority.

Enhance physical security with Kisi

All modern businesses are moving to cloud-based, interoperable, integrated security systems. Adapting to different business needs, these cost-efficient systems are perfectly scalable, automate operations and enhance not only security but also convenience.

Enable seamless coordination and swift decision-making by overseeing your whole security suite —access control, visitor management, video surveillance, analytics and reporting, and intrusion detection — from a single, intuitive interface with the Kisi One Security Platform.

Contact us to find the best solution for your needs or see how other successful businesses like KAYAK, Doctors of BC, Saint Jude Catholic Church and School, and Gather are securing their spaces with Kisi.

KAYAK

Case study

doctors of bc

Case study

SAINT JUDE CATHOLIC CHURCH & SCHOOL

Case study

gather.

Case study

Contact our sales team

Give us a brief summary of your needs and we'll get back to you within one business day

Contact us

45 Main Street,
11201 Brooklyn
USA

sales@getkisi.com
getkisi.com

kisi