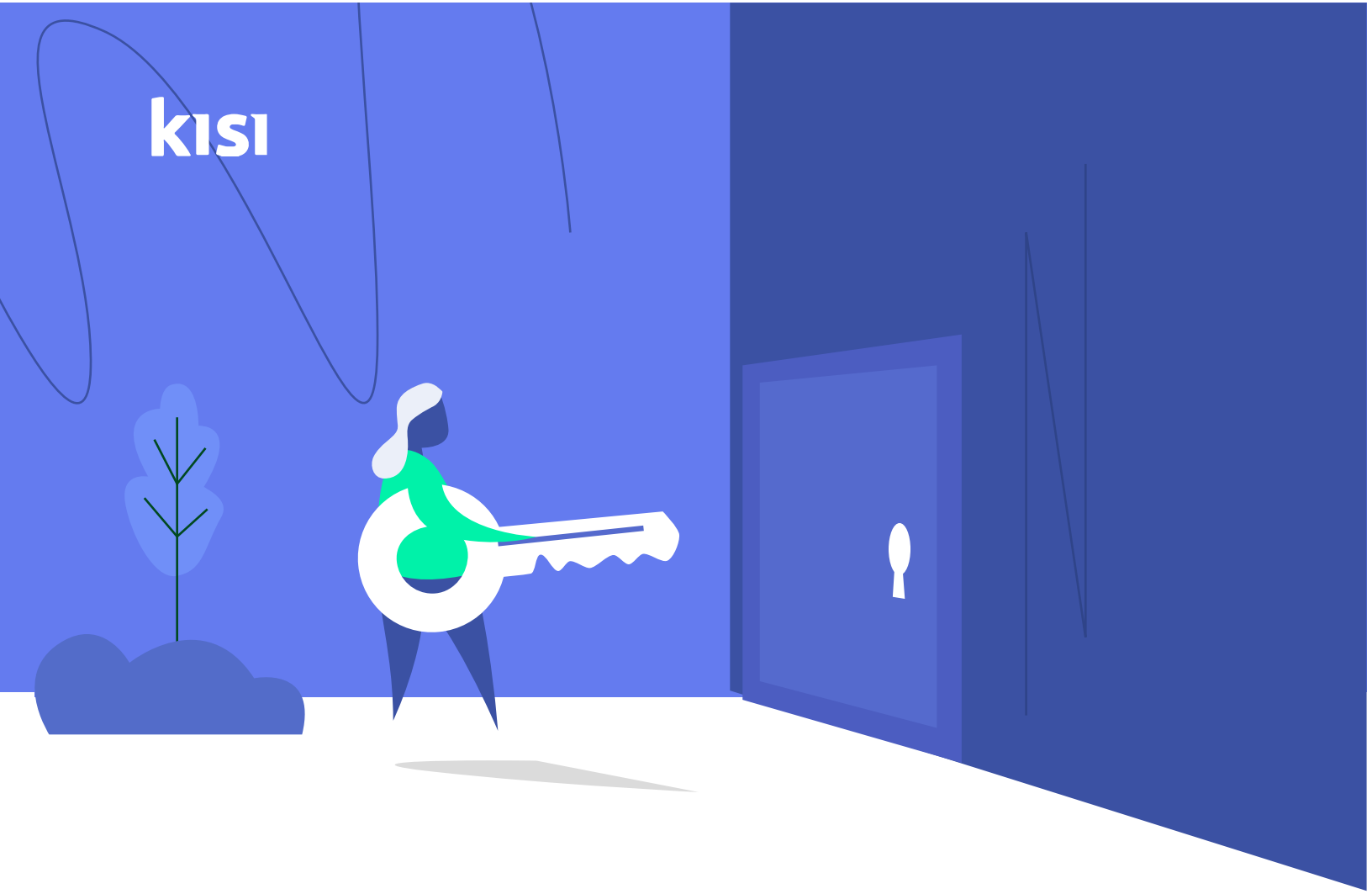
kisi

Ultimate Guide to Physical Security

A guide to getting started with access control

www.getkisi.com



What is physical security?

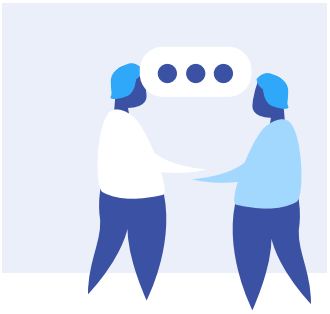
Physical security has traditionally been viewed as an unsexy and tedious topic that few want to tackle; however, everyone knows that safety and security must be adequately addressed. From talking to endless lines of hardware store reps about installing door locks, to antiquated, dystopian visions of bored security guards in rooms with dozens of CCTV monitors— the label of physical security doesn't necessarily inspire passion.

We're here to tell you that it doesn't have to be that way. With cutting-edge technology and the Internet of Things revolution, the world of physical security has drastically changed—making your physical office a safe space has never been easier.

If you're new to the world of physical access control, you might have some questions:

Components

What are the pieces of an access control system and how does it work?



Why Access Control

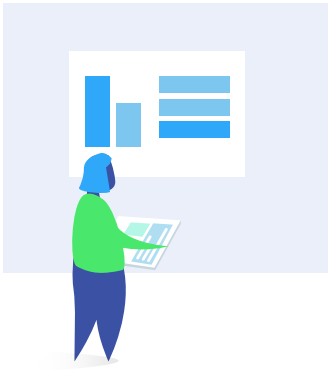
Why do people choose access control?

Quote and Cost

How much should I spend on an access control system and what's a sample quote?

Setup and Operation

How do I set up an access control system?

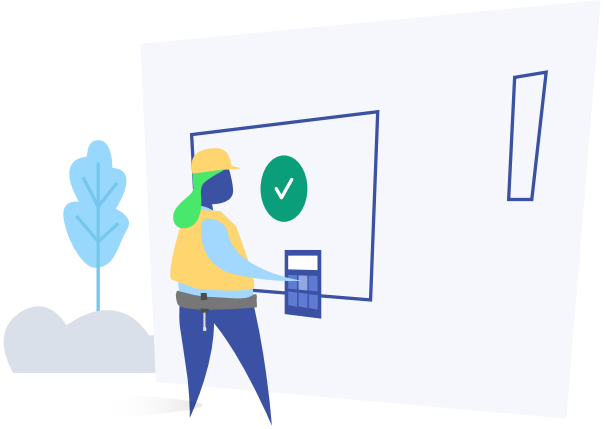


Managing and Using

Who manages the day-to-day aspects of the system?

In this guide, you'll find:

- Curated content from expert sources
- Overviews of the relevant fields of access control, video and alarm systems
- Best practices and recommendations
- Tips on how to incorporate new technology into traditional workspaces
- Various case studies on specific technology and companies that can modernize your office, work-space or facility



Here's an overview of how to find the best security consultant and what to look for.

Free Information vs. Security Consultant

When trying to learn about security quickly, most people call a local security integrator, installer or consultant; however, understanding access control basics is free when searching online or finding a resource like this guide.

Is it absolutely necessary to learn about access control yourself? No, definitely not; however, it will save you a lot of time when your project is underway and people start speaking jargon that freaks you out—especially if it's past the construction deadline, or your employees are arriving on Monday to an office with no access control system.

Introduction to Access Control Systems

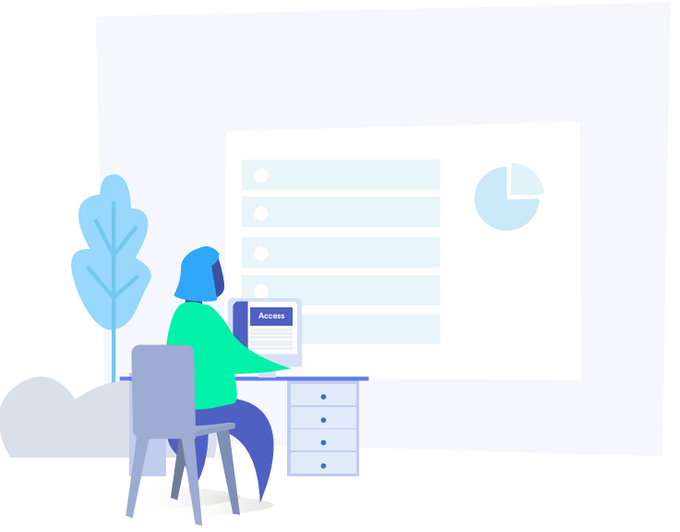
If you carry an access card, ID badge, or keyfob then your office already uses an access control system. But how does it really work? It's difficult to imagine, since most people have never seen the system. When initially thinking about it, most people believe it's just a card reader on the wall.

In reality, there are a few parts behind-the-scenes that make the magic of opening a door possible.

We'll leave you with a comprehensive understanding of how access control systems work and the language needed to communicate about it with vendors.

What is physical access control?

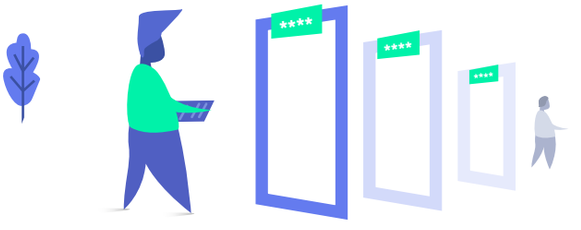
An access control system allows you to manage, monitor and maintain who has access to certain doors and at what time they can access them. The simplest type of access control “system" is a standard deadbolt with a brass key.



Since the introduction of the key, some 4,000 years ago, more advanced systems have been introduced. Today, there are different computer-based, electronic access control systems.

Using an access control system allows you to manage access or entry to almost anything: Files, workstations, printers and—in our case—door, facility, building or office access. The standard form of today’s access control is an “access card,” instead of the key, to grant access to a secured area. For access to larger buildings, the exterior door is managed by the building and the interior, or tenant, door access is managed by the individual company.

Think about a small business located in a larger building: The company will use the access card provided by the landlord to get in the front door. However, it’s often the case that the landlord is not responsible for the specific office security. Thus, the small business might wish to install their own access control on their doors, and a seperate intrusion detection alarm in the office, along with one or more video cameras.



Why do we need access control?

The purpose of access control is to provide quick, convenient access control for authorized persons while, at the same time, restricting access for unauthorized people. Beyond the obvious reasons, there are more reasons why access control should play a significant role in your organization:

Compliance

Some companies need to be compliant with health data regulations (HIPAA) or credit card data regulations (PCI) or even with cyber standards, such as SOC2. The ability to pull compliance reports for access control, on demand, is a huge benefit.

Experience

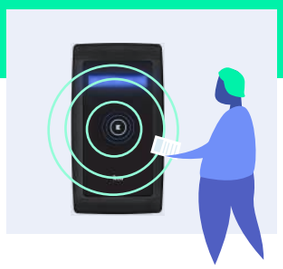
If you have a lot of visitors or clients coming to your space, you might be looking for a welcoming experience at the front door or front desk. Access control not only improves your operations but it’s modern and impressive for visitors to use.

IP / Data

If you’re working in a company on expensive products or sensitive data then you definitely want to control and monitor who enters your facility.

Standard Features of Access Control

Access control systems vary widely in type and complexity; however, most card access control systems consist of the following basic components:



End-User Facing

Access card, card reader and access control keypad

Admin Facing

Access management dashboard, integrations or open API

Infrastructure

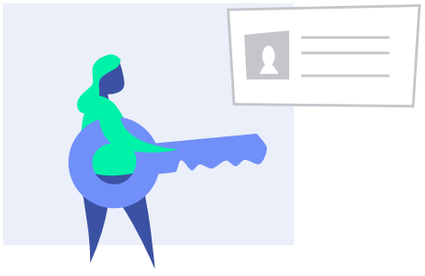
Electric door lock hardware, access control panels, access control server computer and low voltage cabling

The User Facing Side of Access Control

The user facing side—often called “credentials,” extends to access credentials in the form of access cards, ID badges or smartphone-based mobile credentials.

The credentials are whatever physical token you have that will communicate with the reader, as well as the reader itself. The reader here refers to the device on the wall that reads your credential or permission.

Here’s a detailed description of both sides of the end-user facing side of access control:



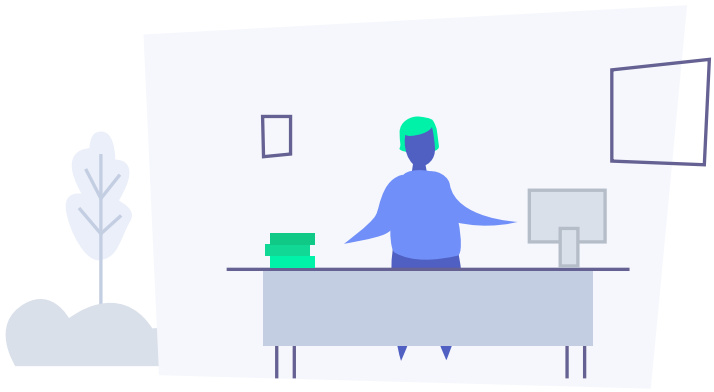
Credentials

This is your electronic “key” and it grants you access. It could be an access card, ID badge, ID card or smartphone-based mobile app that acts as an electronic key. People use one, or a combination of all three, to gain access through the doors that are secured by an access control system. The form of access cards is the same as credit cards, so it fits in your wallet or purse; however, demagnetization is very common with basic access control cards. The benefit of using mobile credentials is that they are personalized, so any unlock event can be tracked back to the person associated with the credential.

Card Reader

The card reader, mounted on the wall, electronically reads your credentials and sends a request to unlock the door (using your user credentials) to a server. Typically, the type of cards used are proximity cards, which require the card to be held in a 2” to 6” proximity to the reader—as opposed to being inserted. Card readers are mounted outside of the perimeter (exterior non-secured wall) and next to the door they should be unlocking. In addition to card readers, some access control systems provide the option of using keypads (PINS) or biometrics, instead of cards or smartphones, as credentials. This is rather uncommon, since PINs can easily be passed on and biometrics are difficult to manage—especially if employees or visitors don’t want to share their fingerprint with your company.

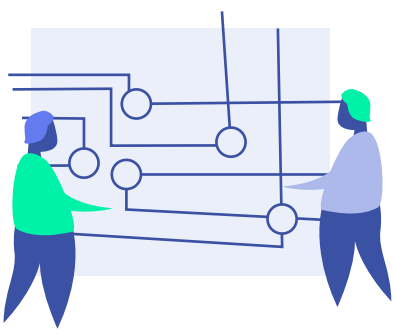
Admin Facing Side of Access Control



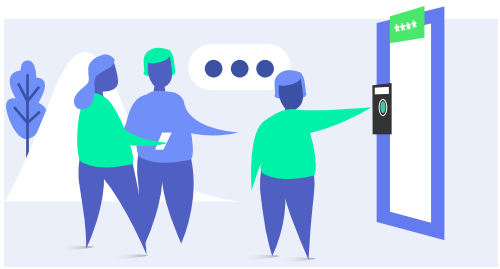
The admin-facing side is where your office administrator, head of security or IT manager sets the parameters on who can gain access and under which circumstances. This involves a management dashboard (often cloud based) and a way to provision access, i.e. a card programming device.

In more advanced systems, the manual operations can be automated. For example, the provisioning and de-provisioning (creating and deleting access) can be done automatically by connecting the access dashboard to your company directory of employees. When a new employee shows up in the system, a new access right is automatically provisioned via a directory like Google Apps, Microsoft Azure, SAML or Okta, among others.

Management dashboards are portals where administrators can manage, maintain and control access for employees, visitors and staff.



API and integrations can be used to automate manual workflows and to make operations less prone to errors.



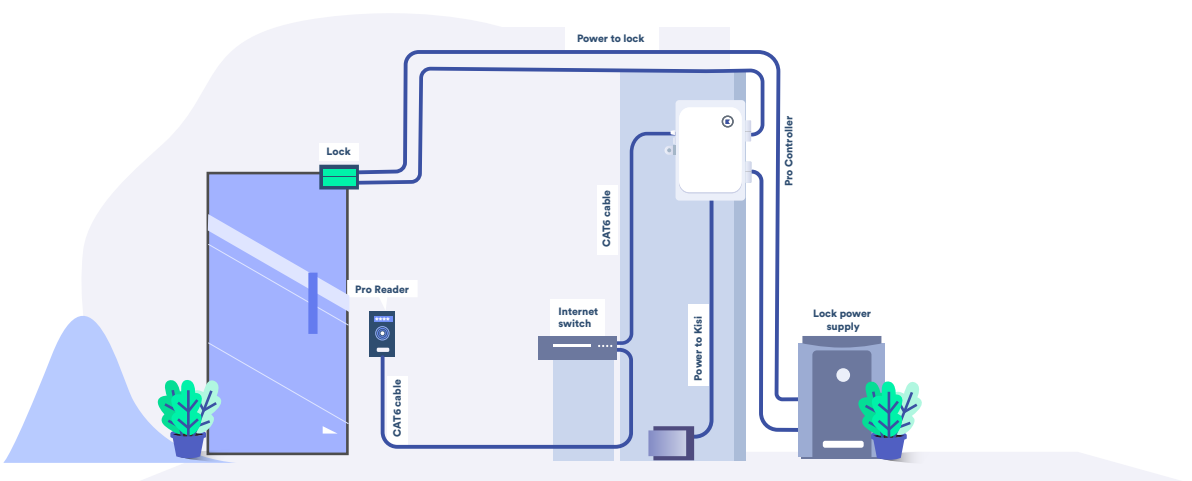
API Integrations

The ability to automatically provision employee access is thanks to the power of API integrations. Rather than reinventing the wheel, many access control systems choose to integrate with other apps that provide added functionality, like single sign-on and active directories, or more niche SaaS tools, like visitor management or member management softwares.

Access Control Infrastructure

Access control infrastructure—the locks, cables, control panel and server architecture—is the most mysterious aspect of the system. The electronic locks are obvious, but what most people don't know is that the locks are all centrally wired to your IT room. This means that a power or signal cable runs from the lock, through the walls, into your IT room where the access control panel sits. The access control panel sends the lock a signal to unlock when it receives the request by the card reader. There are different topologies (as people call it), but for your own basic understanding of access control systems let's just assume this diagram for now.

Here's an overview of Kisi's topology
(or wiring diagram) of a basic access control setup:



Wiring diagram of an access control system

Electronic Locks

Electronic locks are used to electrically unlock the door that they're installed on. Typically, they have a wire that supplies them with power.

Some locks open when power is supplied (fail secure locks) and some locks lock when power is supplied (fail safe locks). The reason for these two different types of locks: In the event of a fire some doors, like your front door, should remain open to comply with building and fire codes—they must allow people to exit the building at any time. Other doors, like an IT room door, are wired fail secure and should remain locked even during an emergency.

In terms of locks, we see everything from electronic strikes, electromagnetic locks (mag locks), electric exit devices, electrified mortise door lock sets, and many more. Based on your door type and construction, the integrator will specify the best lock to install.

Regardless of the lock that's installed, most are wired back to the access control system panel.

Access Control Panel

The access control panel (sometimes called "access control field panel" or "intelligent controller") is not visible to most people in a facility, since it's installed in the IT room, electrical, telephone or communications closet. The reason why the panel is locked away is because all locks are wired to the access control panel. When a valid card is presented to the card reader, the door access panel receives the request to unlock a specific relay, which is connected to a specific door wire. When the relay triggers, the lock is being powered (for fail secure locks) and the door unlocks. This is how the access control panel manages the access activity for building doors. The amount of access control panels you'll need depends on the number of doors that each panel controls. One of Kisi's access control panels, for example, can control up to 4 doors. If there are more, they can be modularly added next to each other.

Access Control Server

Every access control system needs a server where the permissions are stored in an access database. It acts as the center or "brain" of the access control system. The server makes the decision if the doors should unlock or not by matching the presented credential to the credentials authorized for that door. The server can be a local Windows or Linux server, a cloud-based server or even a decentralized server, where credentials are stored in the door reader. The server also tracks and records activities and events regarding access, this allows admins to pull reports of past data events for a given period of time. If a local-hosted access control server computer is used, it is typically a dedicated machine that runs the access software—that's the reason why cloud-based systems recently gained a lot of traction, since multi-facility management can become complicated with local servers.

Low Voltage Cables

Cables, specifically the low-voltage cables used on locks, are often overlooked; however, they're the most expensive part of an access control system when installed incorrectly.

It's important, while building out the space, that all the necessary cables are specified, so that the general contractor knows what to do. If the cables are not planned in at this point, they need to be added later and someone will have to drill into your newly painted walls.

Now that you have an overview of access control components, let's look at a simple access control system:

A simple access control system quote example

Let's say you have an office or building with two doors that are on opposite ends of the facility—like a front and back door.

The office is currently using regular keys to access the door. Management is looking to improve security and operations at this facility by implementing an access control system. They're looking into access control systems because the company is growing and they'd like to have more control.

After taking a closer look at the doors that are security sensitive, the IT room door comes to mind because there are many security-related devices and equipment installed. The door leading from the hallway to the IT room should be secured, as well.

A team member is typically tasked with researching different access control options and getting bids. The team member is researching a few local vendors to contact who supply and install access control. Typically, they will stop by to take a look at your space and the doors, to give you an accurate quote for the access control system. Here is a sample of what a one-door access control system quote might look:

[redacted]

QUOTE

DATE	INVOICE #	CUST #
11/9/2015	0000025032	0000287

SHIP TO: [redacted]

P.O. NUMBER	TERMS	SALES PERSON
	NET 30	[redacted]

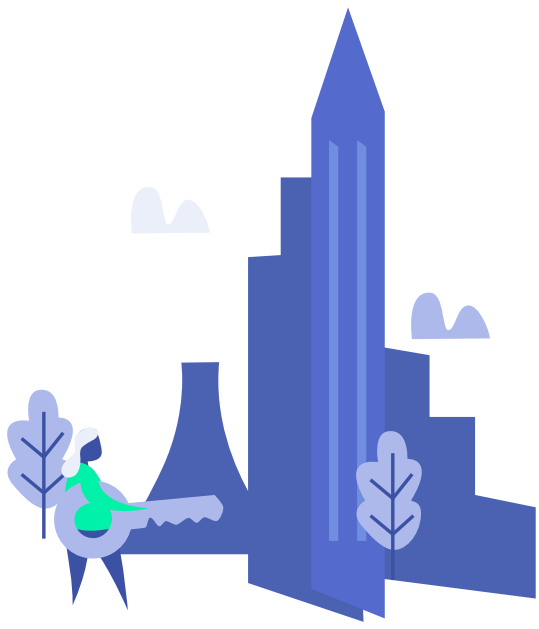
QUAN	DESCRIPTION	PRICE EACH	AMOUNT
	Total Materials		1,856.28
	Total Labor		1,468.17
	[redacted] Fees are INCLUDED for the first twelve (12) months and are collected annually in advance. Cancellation of [redacted] service requires 30-days minimum notice (after initial 12-months). Billing period begins on the 1st of each calendar month.		
	[redacted] Fees for one (1) door will renew at the (Current) rate of $14 per month and are collected annually in advance.		
	Provide and install a 1-Door [redacted] Access Control System to allow access using the Building-issued cards as well as the tenant-provided cards/fobs or mobile devices. Complete turn-key solution is provided, including the electric strike and replacement mechanical lockset on door.		
	Optiona [redacted] MobilePass - allows unlocking of door using the [redacted] mobile app on mobile devices (does NOT require a card/fob). This is an add-on feature that starts at $19 per month for 100 mobile passes. Mobile passes can be revoked and reissued at any time. Account comes standard with five (5) mobile passes that can be used for no additoanl cost		
	SUBTOTAL		$3,324.45
	TAX		$175.55
	TOTAL		$3,500.00

Sample access control quote for companies, like Brivo or others, including a mobile access pass and cloud. access control

The issue is that many installers pack a lot of information into the quote and don't necessarily provide an itemized receipt. There are many ways to gauge the quality of vendors or installers and the quote is certainly one of them.

Returning to our example: The integration vendor conducts the site survey and determines that, in this case, there are three card readers needed for the lock installation of two magnetic locks on the glass doors, and one electric strike for the IT room door. To control the locks, an access control panel is recommended by the installer—it connects the door locks to the Internet.

Also included in the quote is the wiring, to connect everything and set up the system, and a license for maintenance and support that sometimes includes the hosting and a few accessories. Vendors sometimes include a trip charge or service call fee, as well.
Since this example company wants to manage access remotely, a cloud-based physical access control system is recommended. This allows logging on to a web-based portal from any browser, given the correct credentials, to make changes to access rights and share or revoke access remotely.



Remember, the most important thing about a quote is that you get line items so that you understand what is being done and how much each task costs. If the access control installer lumps everything together in one sum, like the example above, they sometimes ballpark the numbers and don't specify the brand of hardware they use. Hardware is another crucial indicator to understand the quality of a quote.

It's important to clarify if the quote includes a Certificate of Insurance (COI); you can ask your building management if you are required to have this for incoming vendors. This makes sure that possible damages by a vendor, up to a certain amount, are covered.

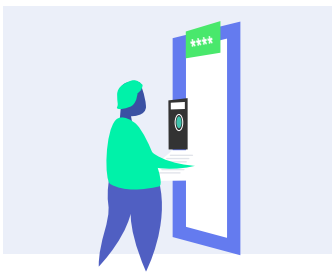
Access Control System Setup and Operation

Once you've found the access control system you like, what happens next? How does the system get installed in your space?

Typically installers take a few days, from confirmation of the order until the actual installation, because they need to order the parts required for the installation. Once you have an actual installation date, you'll find that the installer will do the following:

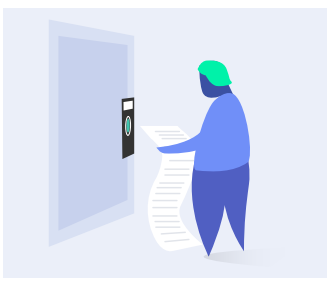
Run the cables

If you don't run the cables you can't connect anything, so it makes sense to start by running the Internet, power and signal cables first.



Install the readers at the door

The reader just needs to be screwed on the wall and connected to power. Some readers, like the Kisi IP reader, need Internet connection and would have to be connected to the Internet for installation.



Setup and testing

If there is a server to set up, it's typically done after everything is installed—so the software can be configured and tested to see that all doors unlock correctly.

Install the access control panel in your IT room

If you have two doors you'll be able to use one access control panel, because most of them can handle multiple doors. The integrator might install a backup power supply, or other additional security hardware, depending on your building's specifications.

Install the locks

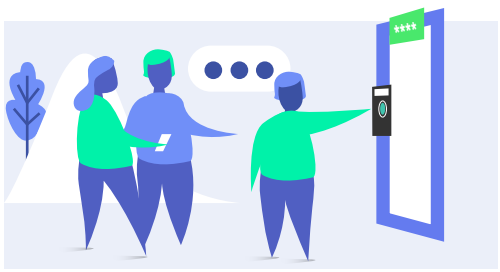
Depending on what type of door you have, the integrator will either install a magnetic lock, electric strike or electrified mortise lock. This might involve cutting into the door frame, which is why sometimes it makes sense to do this step first so the office workers are not annoyed in the middle of the day.

Migrating and Introducing the Access Control System

You should run through the following steps, once you have the system set up, to roll out access control to your organization:

Set up a door access schedule

When should certain doors unlock? Which types of access groups or individuals should be able to gain access? The door access schedule can become political: Are IT managers allowed to access all doors? What about executives? Are they allowed in the office 24/7? It's a good exercise to discuss this with your security, facility and management teams, since these are the rules that your strategy will be based on and it will determine what you actually want to control.

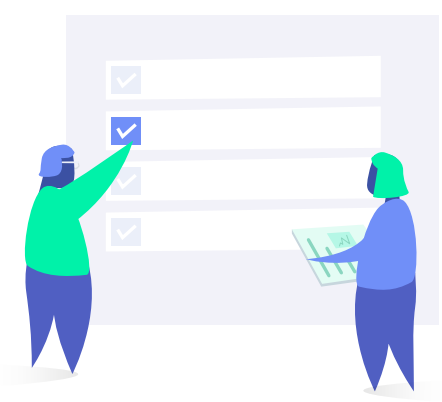


Test the system with a few pilot candidates or coworkers

Try running through the process that you envision for every employee or visitor with a few, at first. Provision access for them, activate their access, hand over the access card or share mobile access with them, then see if it works. If you roll out your process too quickly, you might have some smaller hick-ups and the more people you involve, the faster the problem multiplies.

Set up the rules in your access control software and test if they work

Now, under certain conditions, you want the user not to be able to unlock the door. Run through all possible scenarios. Many offices get broken into during vacation days. Some offices automatically unlock their doors during work days. If the work day is a public holiday, burglars know they might just be able to walk in.

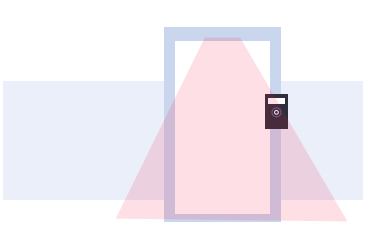


Announce the roll-out

Send an email to everyone to announce the change in access control. People don't like change—some might have an emotional bond to their physical key, so be ready for push-back and highlight why this makes your workplace safer and your company more secure.

Onboard your team

Once the system is tested, announced and approved the fun part begins: The actual roll out. You can start provisioning access for your team. The most important part to consider is that some people will have issues or problems getting access, so make sure to roll out on a day that is not the most critical. Most people choose Fridays so that there's time to troubleshoot.



Door Status Monitoring Feature

Automatic Unlock Feature

Reporting Feature

Check out Kisi's product pages for more advanced features:

- Kisi Access Reader
- Kisi Cloud Access Dashboard
- Kisi IP Control Panel
- Kisi Mobile Credentials.

Alarms

An alarm is a device that emits some sort of attention-grabbing audio-visual signal when its alarm conditions are met. These conditions generally relate to some sort of issue or anomaly in the environment of the alarm. Alarms come in many forms—loud siren, silent, fire, burglar, smoke, etc. All alarms mentioned here track some parameter of their environment, and when a change occurs, they notify the administrator of said change.

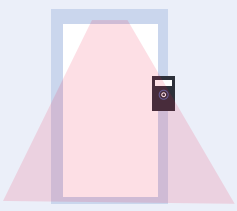
The reason we need them should be straightforward. While incidents are uncommon, the difference in consequences between being notified of one as it occurs, and only learning about it after the fact, can be dire.

Consider the difference between being alerted to a burglary in your office and having the police stop it, versus coming back to find everything of value gone. Or the difference between being alerted to a fire developing next door, and having time to escape, versus not realizing it until it's too late.

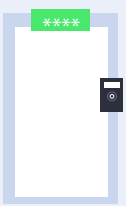
Alarms of all kinds are integral to the livelihood of an office and, as such, are one of the three most foundational aspects of physical security.

In this section, we'll cover different types of alarms, discuss the infrastructure needs, and give a brief glimpse into the future of alarm systems.

Different Types of Alarms and How They Work



Fire Alarm



Burglar or Intrusion Alarm
Door and Motion Sensors

Integrated Alarm Systems

Fire Alarms

Fire alarms are arguably the most important type of alarm you can have in any space. Forget about loss of equipment or information, what is at stake are the lives of your employees. Having a functioning and competent fire alarm is not only paramount, but also required by law in every state.

They typically come in two forms: Manual and automatic alarms. Manual alarms are, typically, those visually prominent red "fire" boxes you see along the walls that incorporate a handle of some sort that you can pull.

While these are undoubtedly important in any office, employees can pull them preemptively, and automatic detectors are not perfect—that's why we will mainly concern ourselves with smoke alarms.

Smoke Alarms

Automatic smoke alarms usually come in two varieties: Smoke and heat sensors, while some systems offer both. Alarms can only detect the by-products of fire—smoke and heat; AI image recognition technology is not quite commercially available at the level where a camera could reliably detect flames, yet.

In general, though, most fire alarms are smoke detectors, and these are preferred to heat detectors. While heat detectors are certainly cheaper (they require far less maintenance and replacement than smoke detectors, and are essentially a glorified thermostat), they fail at detecting smoldering fires, or low heat ones.

Often, an office fire will not be a blaze, but instead a slow burn of some plastic or other synthetic material. These will not give off enough heat for any detector or human to notice, and sometimes may not even emit visible smoke, but they will emit noxious gases like carbon monoxide (deadly and odorless) that are far more dangerous. Most fire-related deaths in the U.S. are caused by inhalation of toxic fumes, rather than all out fires. Heat sensors cannot detect these, but all modern smoke detectors can, so you'll probably want to opt for one (per room!) of those in your office or residence.

Motion Sensors

Unlike door and window sensors, motion sensors can be set up anywhere in your office or home, and as the name suggests, they are triggered by motion in their line of sight. You might set these up in discreet places, like at the foot of a door, where someone entering would necessarily trigger it, or if it has a wide view, simply in a top corner of the room where it can get a bird's-eye view.

The motion sensors you'll want to look at are called Passive InfraRed (PIR) sensors, and they fall in one of two types. Either a tripwire, or a general heat detector. For a tripwire, the idea is simple: There are two devices installed at ankle height on either side of a door: An emitter and a receiver. The emitter sends out an IR beam, invisible to the naked eye, and the receiver constantly registers the signal. However, when someone steps across the beam, the signal is interrupted, and the receiver pings the main alarm panel. These sorts of sensors are especially useful at points of entry and egress to sensitive areas. Heat detectors, instead, will be installed in a spot with a good bird's-eye view of a room. They span a continuous region, being the whole room, rather than a straight line, and rather than an emitter and a receiver, the primary device doesn't emit any IR light, merely registers ambient IR signals.

The crux here is that infrared light is emitted by any body that emits heat, so if any warm body (read: any person) enters the room, the heat signature of the room will change, and the sensor will detect this and trigger the alarm panel. These sorts of sensors can be used in conjunction with the tripwires, and add a layer of security to a room when an administrator wants to monitor its usage. Unfortunately, the nature of these signals is that they are rather murky, especially with most commercially available systems, so while you will be able to tell if there is a person in the room, you generally won't be able to tell how many people are in the room, or any sort of granular data on size/shape of the intruder.

Cabling

Much like for access control, the cabling is an often overlooked, yet crucial, component of any alarm system. Refer back to the access control section for a more thorough exploration of this, but you will not want to overlook this crucial step in the installation lest you find yourself having to drill holes in your newly renovated walls.

Infrastructure and Hardware

Here's an overview of the type of hardware you would need for modern alarm systems and how it works. Alarm systems typically consist of an alarm panel, door, window and motion sensors, as well as cabling.

Alarm Notification Types

The first, and most outwardly evident, aspect of an alarm system is the alarm itself. Whether it be the blocky red manual fire alarms or the sleek, discrete motion or contact sensors, these will be the most user-facing devices in any integrated system. As such, you will likely want to optimize for ease of use and recognizability with respect to the most salient aspects of the particular alarm.

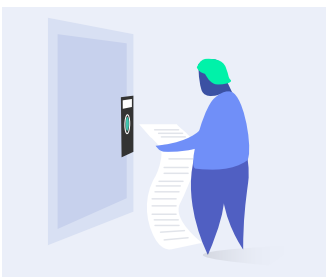
For fire alarms, in the case of a roof smoke detector, even though aesthetics are important it is usually advisable to have it be evident which is the fire alarm, to prevent employees from accidentally covering it up (in which case it would no longer serve its purpose). Burglar alarms, on the other hand, will often warrant a certain measure of discretion and hiding, especially in the case of those trip wires that are specifically meant to not be seen.

In any event, we recommend going over your floor plan thoroughly with the installer before making any sort of decisions as to the placement and installation of the alarms.

Alarm Panel

The alarm panel will be, again, the metaphorical brain that controls all of your alarm systems, as well as the main interface that you will interact with. Traditional alarm panels have the familiar keypad where you can input your code to disarm the alarms, whereas more modern ones will feature a touchscreen with a more developed and sophisticated UI.

The alarms, as stated above, are essentially just sensors. They accomplish a particular function, be it sensing levels of smoke in the air, or whether an IR beam has been tripped, or whether the general heat signature of a room has changed, but they can do little more than send this signal to a given server themselves. This server will be the alarm panel, usually installed in an IT closet, or other secure location that only an administrator will have access to.



We will discuss the distinction between monitored systems and self-monitored later in this section, but to give a preview, the alarm panel will be where this distinction is put into effect. If the system is self-monitored, then the alarm panel will comprise the user interface for the administrator to operate it. Meanwhile, if it is externally or automatically monitored, the alarm panel will establish a communication with the relevant third party, and coordinate with it to run the alarms, and make sure the system is running up to standards.

Door and Window Sensors

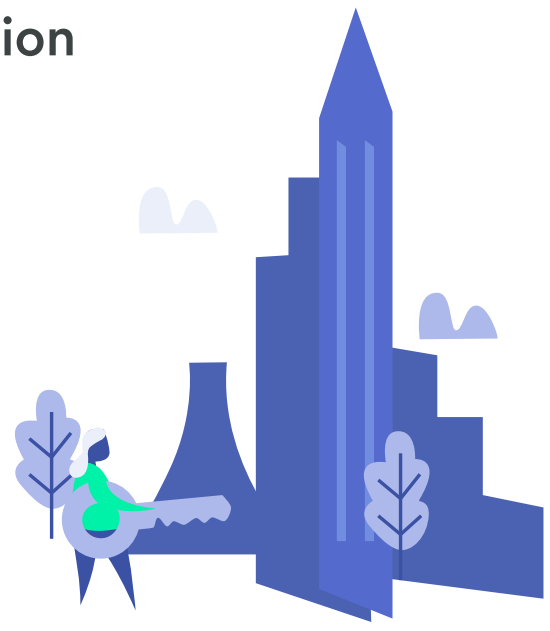
The first of the two categories is that of door and window sensors. As their name would indicate, you would install these on your doors and windows, and they detect any time said door or window is opened. They are comprised of two parts, one which is installed on the stationary part—like the door or window frame—and one on the mobile part. They can be either wired or wireless, depending on the model you opt for, but by design both need electricity, so wireless ones will need battery replacements.

The way they accomplish this is deceptively simple: They use magnets. Rather, they use an induced magnetic current running across the gap between the two parts of the sensors. They run an electric current from one side to the other, so naturally when the door/window is opened, the connection will be interrupted, and this will trigger the sensor. The sensor then communicates with whatever alarm panel it's set up with, and a notification is sent to the administrator of the system.

A variation on this is a door-held open alarm. These are the same sorts of sensors described above, but instead of sounding the alarm when a door is merely opened, they will sound it when the door is held open for more than a given span of time. These require a certain amount more infrastructure inside the sensor itself, as they need to be equipped with a timer, but beyond that the process is inherently the same.

Brand	Description	Cons
CPI Security System	Provides home, business and commercial door alarm systems. It's a local enterprise that operates in Georgia, Virginia, North and South Carolina, Tennessee, Alabama, Florida and Maryland. The company is touted to have a local touch and a closer business relationship with the police and the fire brigade than nationwide providers. Security is monitored from the headquarters in the Southeast.	-Clients are bound to a 60-month contract -To terminate or discontinue services a 60-day written notice is required. -End users often complain about poor customer service
Simplisafe	A customizable DIY home security system. Let's have a look at how it ranks among other access control alarms and whether it can be used as one of the alarm systems for business.	-Frequent connection issues from devices to the monitoring system -Prone to giving false alarms. -Simplisafe is battery-powered, a dead battery means security system failure. -No smartphone app
LiveWatch	Provides home monitoring , and also specializes in security systems for small businesses.	-No 24/7 customer support -Wireless technology can experience connection issues -Use same equipment in 2018 as in 2015 -Some complain the alarms can be triggered by animals
Getsafe	Provides smart alarm systems for businesses looking for simple, easy-to-install alarm kits, and for homes in need of do-it-yourself modern security and automation solutions. The commercial door alarm system is ideal for small and family-run companies since it's based on a starter kit connected to a mobile app.	-Incompatible with other access control alarm systems -32 user maximum -Not ideal for large alarm systems for businesses
Vivint	Offers intelligent security alarm systems for business and homes. Its real-time access control alarm system is powered by 24/7 remote alarm monitoring. The home security solution of this company consists of access control alarms, CCTV camera, home automation, energy management and commercial door alarm systems.	-Pricey -Charges additional fees for installation -No 24/7 support -Long and complex contracts -Buggy mobile application
Guardian Protection Services	Offers access control alarms and fire systems to residential homes and businesses, as well as intrusion prevention.	-Additional installation fees -No 24/7 customer support -No flooding alerts -No alerts for natural gas leaks & power failure
Protection1	Offers video alarm verification and other security technologies for residential and businesses. Clients have enjoyed the best technology in access control alarms at affordable prices.	-Inefficient support system -Additional installation fees
ADT	Provides a variety of home security and alarm systems for businesses, ranging from wireless and hard-wired systems, to video surveillance, voice-enabled home automation, and connection with third-party services. Customers use a mobile app to manage it.	-Long-term contracts, all plans are for a minimum of 36 months -Customer service depends on the local dealer -Slow response time
Vector Security	Provide robust and professional-grade alarm systems for business and households. Services include the monitoring of burglar, fire, carbon monoxide, environmental hazards and emergency access control alarms generated manually or automatically.	-Poor customer support -Complex service cancellation policy -Ambiguous contract procedures -Relatively high monthly charges
Alarms R Us	A NYC-based provider specializing in commercial door alarm systems for businesses, residential properties based on the Honeywell remote mobile app technology. The basic model can be combined with a CCTV, intercom system and 24-hour monitoring service to guard properties from intrusion, fire and flood, and to enable light and heat home automation.	-Advanced alarm systems for businesses not included -Limited warranty -No power failure alert -Location-limited

Burglar Alarms & Intrusion Detection

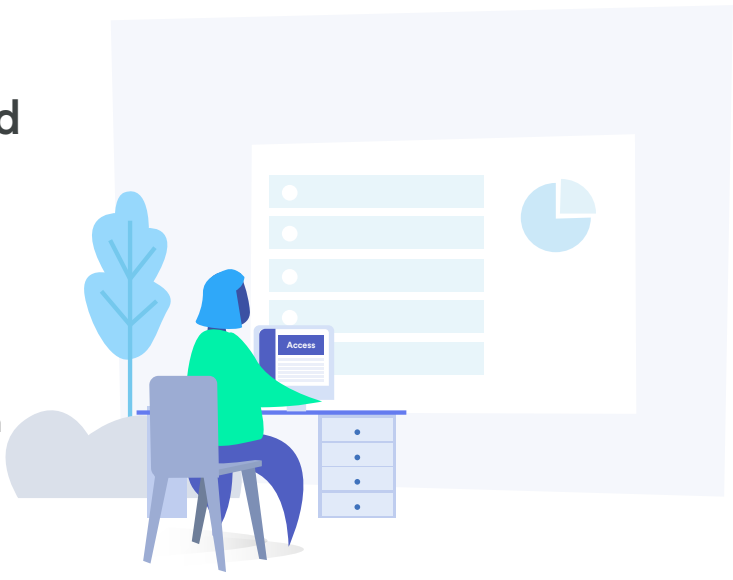


Besides a fire alarm, it is evident that you will want some measure of protection against unwanted visitors entering your space and stealing, or otherwise damaging, property. This is where burglar alarms come in. However, picking the right burglar alarm for your space can be tricky: How will some device be able to tell when an intruder has entered the space? How will they differentiate them from normal employees, and more fundamentally, how do they even determine that they should be notifying the administrator that they've been triggered?

The latter question we will explore soon, but to answer the former, we must turn to the question of timing. An administrator will have to set up the alarms, and in setting them up, she will determine their hours of operation, so to speak. The IT admin will establish at which times the sensors will fire an alarm if activated. For instance, if they are equipped at the front door to the office, then they should not be alarmed at all hours of the day, because normal traffic in and out will constantly trigger it. Therefore, it should only be alarmed when nobody else is present, in other words, outside of normal work hours. However, if they are equipped in super-secure server rooms, where nobody is ever allowed except for the IT admin, then they should be constantly alarmed. These are decisions that need to be taken when the alarms are installed, but they can easily be amended later on, through the UI of the alarm itself (generally a controller box or a web interface, depending on how modern of an alarm it is).

Burglar alarms generally fall into two main categories (excluding security cameras, covered later in this guide)—door/window sensors, and motion sensors. Door and window sensors are installed at points of ingress to space, whereas motion sensors come in a couple of different types and can be installed throughout the office. In the infrastructure and hardware sub-section of this alarm section we will explore those two, their pros and cons, and when they might be right for you.

Integrated Systems: Door Forced Open Alarms

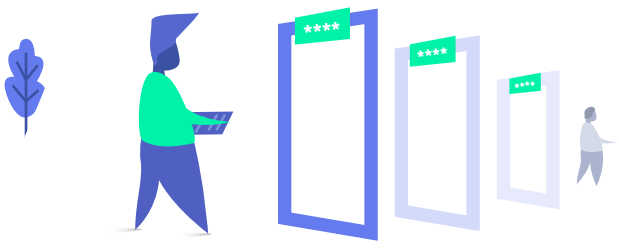


These last types of alarm are mentioned separately as they require a more significant investment in terms of infrastructure: They require you to have an integrated access control system equipped on the door (for our own integrated solutions, click here). Access control systems were covered in the first section of this guide, so I will not belabor the point here, but the alarm portion of these systems is similar to the door sensors described previously, except that they communicate with the door access system and only raise the alarm when the door is forced open; when it's opened without the access system having granted permission.

> In most cases, a user will request access from the system, be it through a door reader, or a request to exit button, and the system will grant access (if the credentials are cleared), thereby unlocking the door and, crucially, communicating to the sensor that the door is expected to open. This will make it so that the sensor doesn't trigger the alarm when the magnetic current is interrupted. However, if the access system had not told the sensor that a door opening event was to occur, the sensor would interpret the door opening as a "forced open" event, and trigger the alarm.

These sorts of sensors can be incredibly useful because without them, an IT manager will receive a notification every time a door is opened, and the vast majority of these open events will be normal employees or authorized personnel on routine business, resulting in a lot of noise that relevant, important alarms (such as an intruder using the door) might get drowned out. Of course, these systems are more expensive, requiring an access control system, but hopefully after reading the first section of this guide that won't seem so daunting a task to you!

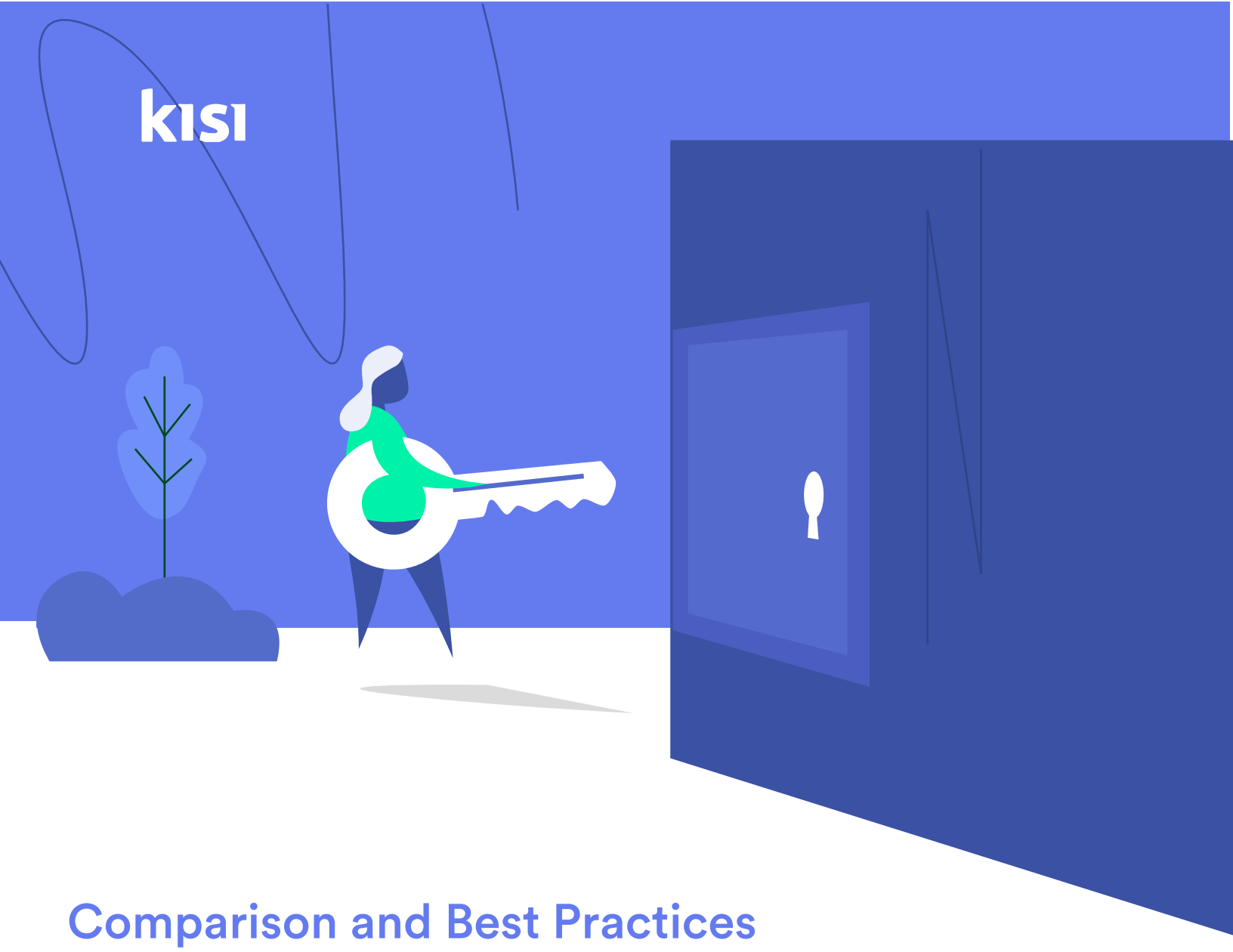
Open vs. Home Alarms



A question that comes up often regards the distinction between an office alarm system and a home alarm system. After all, we've been agnostic about location-casting most of the sensors and gadgets that have been discussed. That's because the only difference between an office and a home alarm system is general scale, and preferences of the particular administrator. There is no inherent difference in manufacturing process or purchasing, aside from what the buyer feels is right for their space.

Concretely, this means that for most small offices, the systems you install will largely resemble a home security system, with perhaps the added occasional security camera, or reinforced door lock for a server room. The intrusion sensors, fire alarms, door locks, etc. will by and large be the same ones across most similarly-sized spaces.

If you're seeking to secure an entire skyscraper of offices, or a large apartment building, the requirements will be different from those of a family home or 20-person office. However, the main differences will be in scale, and not in type.



Comparison and Best Practices

Monitored vs Self-Monitored Alarms

Based on the type of alarm system you have, you'll want to make a conscious decision about whether you want to self-monitor it as an IT or operations manager, or whether you want it to be monitored by an external third party—like the company itself, or an automated system.

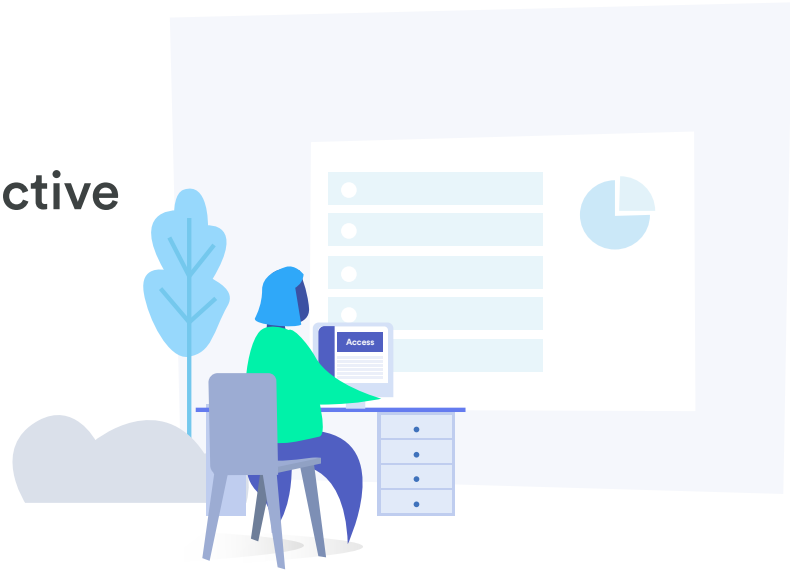
We would highly recommend assigning a fire alarm to exterior monitoring. This should seem obvious: If there's an actual fire in the building, the administrator won't have the time to go in search of the IT cabinet/alarm panel and run the alarm protocols. Therefore, you'll want an automatic monitoring service to receive the signals from the fire alarm, do some basic (and quick!) false alarm control, then trigger the systems and get the building to evacuate.

Now we can move on to burglar and intrusion alarms, where the choice actually exists. In general, monitored services tend to be more reliable, with false alarm detection, quality controls, failsafes, and backups, but they are usually costlier (with licensing fees), and less flexible/configurable, coming in pre-established pack sizes. As a general rule, a larger building with more doors, and more to lose, will want to go for a monitored system with a trusted, established company, whereas a smaller or more niche business might want a more versatile and self-monitored option.

Some of these systems might lend themselves to self-monitoring, but most of them all but require automatic monitoring. For standard door and window sensors, in any office with more than a couple of employees and one door, if the sensors are constantly on then some sort of automatic tracking system should be employed. Otherwise, an IT admin could see herself sifting through hundreds of opening events a day, which is simply intractable. Some sort of automatic pattern analysis, certainly available commercially, would be advisable here. Even for door and window sensors that are only active on the "off hours," so to speak, some sort of external monitoring might be the right call. Indeed, if an unauthorized and irregular access happens at night, and the IT admins are asleep, they'd still want the break-in to be recognized as such, and for the alarm to be triggered. The same sort of logic applies to motion sensors, and to door forced open sensors.

In general, despite the sometimes elevated recurring costs of a monitored system, our recommendation would be to make the leap and spring for a professionally monitored system if you want your office truly secure with 24/7 response times.

The Future: Sophisticated Security Systems and Predictive Data Analysis



While security systems are certainly advanced and provide a high level of safety, unheard of up to a few years ago, the future of the industry is very exciting. We will first explore the emerging, interconnected sophisticated systems appearing, and move on to our favorite topic, predictive data analysis that's automatic.

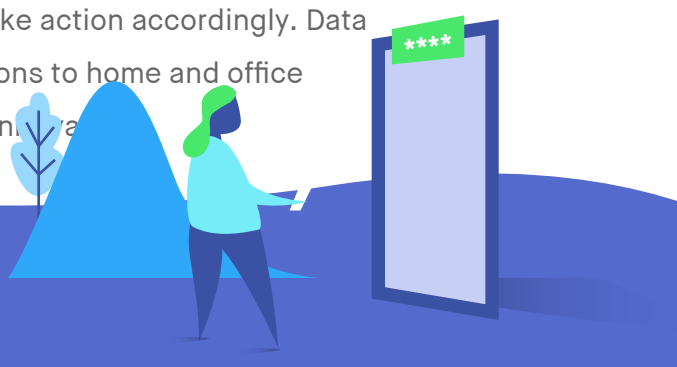
Connectivity

Connectivity is the hot topic in home and office security; the most modern offerings are integrated systems, where each component of your security suite communicates with the others. This way, they are better able to track activity and use of the office/home, and provide you with more comprehensive and fool-proof security. To give a straightforward example, if your fire alarm is connected to your access control system, then in the event of a fire, the alarm can tell the door controllers to unlock all the doors, allowing employees to exit the office more quickly. Similarly, if your motion sensors are connected to access control systems, and they detect an unexpected movement in the office, they can tell the doors to lock themselves—either preventing further burglary, or even locking in the burglars while the police arrive.

Data Analysis

Another rich path of innovation, on the back end of these systems, is the increase in complexity of the data analysis algorithms that track your office security data. As I discussed in the monitored vs self-monitored section, the best security systems for larger offices will be monitored by third parties (the security companies themselves) and innovations in data algorithms for monitoring will make these even more effective. A prime example is the door and window sensors: As I've discussed, for an office of any size there will be dozens, if not hundreds, of opening events for any door you'd want to have a sensor equipped on—so it would be useful to have it monitored by an automated system. With the more sophisticated modern algorithms, though, beyond just telling you if a door opened at an unusual hour, they will be able to tell you, for example, if the door opened an inordinately high amount of times in a day—possibly indicating that the office is over-crowded, and prompting you to take action accordingly. Data science is a very exciting field, and its applications to home and office security present some very appealing paths to in[illegible]

Here's the second part of our physical security guide—the next topic is the one missing element of future security innovation we haven't discussed yet.



Video Surveillance

In this section, we'll cover a crucial aspect of physical security: Video surveillance. It's important to note that this does not just limit itself to the classic CCTV camera monitors stacked on top of each other, with poor quality, and two confused guards trying to track a burglar. This extends to everything from a private camera on the porch of your house to modern, sophisticated IP cameras that perform data analysis and can track employees around the office with facial recognition to accomplish an audit. I'll survey the most popular types of cameras out there, and then give overviews of the modern features you might expect to have in a good one.

Why invest in a video camera system?

Cameras provide the added benefit of tracking your employees to detect and document events. Often, this is used for audit compliance.

A video camera system might, at first glance, seem like an unnecessary luxury, but if properly utilized, it can make a big impact in helping secure your space. The intruder alarms that I've been discussing so far are all well equipped to detect when an unwanted visitor enters the home or office, but they all fall short in one notable category: being able to tell who it actually was who broke in. After all, if the intruder manages to get away with stolen property, how can you possibly expect to recover it if all you have is a hazy heat signature from the intrusion?

This is where security cameras come in. The idea is certainly not a novel one - security cameras, in some form or another, have been around for decades, ranging from the clunky old CCTV systems with the classic image of a security guard in a room surrounded by pixelated monitors, to modern sleek HD solutions. Today, they come in many shapes and sizes, with some solutions more adapted to small offices or homes, and some to large buildings, but the fact remains that for a truly secure office, security cameras are a must.

Types of Security Cameras

In this first section, we'll cover the main types of security cameras—fixed cameras, PTZ cameras, hemispheric/fisheye cameras, multi-directional cameras, covert cameras, and dummy cameras. In the next section we'll move on to the different features to look for within these types of cameras.

Fixed Cameras

Connectivity is the hot topic in home and office security these days, with the most modern offerings being integrated systems; this is where each component of your security suite communicates with the others. This way, they are better able to track activity and use of the office/home, and provide you with more comprehensive and fool-proof security. To give a straightforward example, if your fire alarm is connected to your access control system, then in the event of a fire, the alarm can tell the door controllers to unlock all the doors, allowing employees to exit the office much more quickly. Similarly, if your motion sensors are connected to access control systems, and they detect an unexpected movement in the office, they can tell the doors to lock themselves, either preventing further burglary, or even locking in the burglars while the police arrive

Dome Cameras

They offer much the same features as a box security camera, comprising camera, lens, and mount all together, but offer the advantage of being sleeker and more aesthetically pleasing. In addition, given the dome over the camera, they offer protection from the lens both from environmental factors and from vandalism.

Bullet Cameras

Bullet cameras are essentially more modern and sleeker versions of the box cameras. They also combine camera, lens, and housing in one package, but generally also include IR illuminators for low lights, and offer a much smaller footprint than the box cameras. Generally used for low light environments.

PTZ Cameras

These cameras, unlike fixed cameras, offer pan, tilt, and zoom features, enabling you to survey a much wider swath of the room, and zoom in on areas of interest. Depending on the particular model, you'll almost always be able to control its movement via joystick, and some even offer an auto track feature. These will be equipped with rudimentary motion tracking systems, as described in the previous section, and upon detection of motion, track it and continuously record. This feature becomes incredibly useful in the case of any sort of break in where the criminals are familiar with the space and might seek to avoid any fixed security cameras.

PTZ cameras might come in an open format, similar to an articulated bullet camera, or they might also come in a dome, akin to the fixed dome cameras, making them environment and vandalism proof.

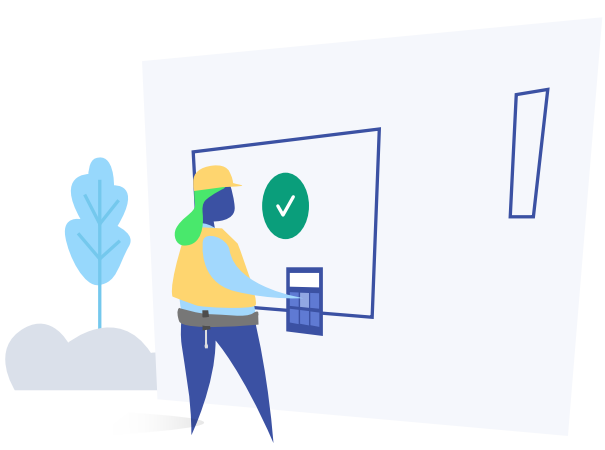
Hemispheric / 360 / Fisheye Camera

While PTZ cameras do allow you to track movements on the ground and keep track on a wider area than fixed ones, it does share the same limitation as them, being a limited specific field of view. Of course, you can follow an individual from one side of the room to the other, but if there are two people on opposite sides of the room, you will only be able to see one at a time. That is, unless you have a hemispheric/360/fisheye camera. Known by any one of these names, this camera is similar to a fixed camera in everything but the lens, which is where its main innovation is: the curvature of the lens grants it a wide field of view, often able to encompass an entire room.

The utility of this cannot be overstated. You can, for instance, install one of these at a corner in a hallway, and in one continuous image monitor the entire hallway. Or you could install two at opposite corners of a room, and have a failsafe: in case one of the two malfunctions, or is tampered with/covered, you'll still be monitoring the whole room. While they are generally pricier than fixed cameras, given the particular design of their lens, they could certainly be worth it for your space.

Multi-Directional Cameras

Multi-directional cameras allow you to view a wider area, much like 360 cameras, but accomplish this by stuffing multiple cameras and lenses into the same enclosure, rather than having one wide-angle lens. They provide much the same benefits as a wide angle lens, but the main advantage to this method over the former ones is that fisheye cameras tend to distort the image, in certain cases making it difficult to decipher the image, whereas a multi-directional camera, despite the elevated cost, will leverage modern technology and multiple lenses to combine the video from multiple cameras into one smooth, continuous, non-distorted feed.



Covert Cameras

As the name suggests, covert cameras are a general category of camera that is meant to be inconspicuous, in case you don't want the casual passerby to know that you have a camera installed there. This can be useful in many situations, but in practice, is mainly used for home security systems, in a sort of front lawn/porch area, where it's not immediately evident that a security camera might be there. In an office, most vandals would expect there to be a security camera, and modern anti-vandalism methods would prevent tampering, so would-be robbers would have to cover themselves or cut the power altogether to avoid them, and would be prepared to do so. However, in a home, or anywhere else that a camera is not expected to be, installing a covert camera might be a smart move.

Dummy Cameras

Finally, the last type of camera here is not even a camera, but a dummy; made to look like a real security camera, with some blinking lights or a company sticker, it's nothing more than a plastic or polycarbonate shell. It might seem that installing these is a foolproof way to increase security: They're cheap, easy to install (no wiring), and would deter most petty thieves. However, don't be fooled: To the trained eye, they are easy to distinguish from the genuine article. They might even give those criminals confidence: If they see and recognize that you have a fake security camera, they will likely know that you have no real security cameras in place, and might be more likely to attempt a burglary. In most cases, they are more help than hindrance, but we would recommend not putting too much trust in them.

Features to Look for in Modern Security Cameras

In this subsection, we'll switch from discussing different types of security cameras and focus, instead, on features that each of these types could have that you might want equipped when installing a camera in your space. The first few will deal with software components, centered around IP connectivity, and the last few will be more about the hardware of the camera.

📌 Wireless IP Connectivity

The vast majority of modern security cameras use IP (internet protocol) connectivity technology, and many later features hinder on this element. This means that the information is transmitted as if the camera were a computer, and will be measured in megapixels and transmitted over the network, rather than through traditional cabled solutions. There are many advantages to this: They are more secure, the same amount of security as your network, rather than relying on antiquated cables. Furthermore, the quality can be drastically better, as IP solutions can transmit data at much higher rates.

Also, they are easier to install, as the only cable that needs to be installed is the power, and even then if you opt for a wire-free one and use batteries, you can eliminate wires altogether. Finally, and perhaps the best part, they offer so many more options for data analysis. Given that the video data is being transmitted to a computer, rather than a simple DVR, the computer can then analyze that footage, and glean all sorts of insights from it.

📌 Compression

A notable benefit that IP cameras offer, which aids in the quality of video mentioned previously, is data compressibility. Analog security cameras communicate their feeds directly to monitors via wiring, but modern IP cameras, given that they're run over the network, can compress their feed and thus send much larger packets (read: more pixels, higher quality video) to the computer. The obvious benefit here is that you will have a much easier time distinguishing features in the video, and you'll have none of that antiquated pixelated feed that you see in older TV shows or movies.

📌 Alarm I/O

Another feature available with IP cameras is Alarm I/O. This means that you can either physically plug in, or virtually connect via the network, alarm systems to your security camera. This integration is extremely useful. For starters, many security cameras take a lot of energy, or a lot of data to record, despite the compressibility. Therefore, to be able to hook them up to a motion sensor, such that they only start recording when the motion sensor is triggered, and record any potential theft, would be very helpful. They would be connected to the sensor, which would relay information to them, and then they would be relayed into the alarm panel, where they send their data.

The uses aren't limited to that, though. With modern video analysis techniques, the cameras themselves can be the source of the alarm, and communicate to the panel that an individual is in the space at an unusual hour; or, with facial recognition, that an unknown intruder has entered the field of view. The ability to integrate your security camera with your alarm systems is key, and definitely a feature to be on the lookout for.

📌 Voice Commands: Smart Home Integrations

In the same vein as alarm integrations, many modern security cameras offer integrations with smart home automation systems like Google Home or Amazon Echo. Through the main control pod of these you can run the security camera and issue it commands via your phone or simply by talking. The benefit of this doesn't simply lie in the increased ease of use of your security camera. In a fully equipped smart home, you can control all aspects of your physical security through the main hub. You can take immediate action, based on the information garnered from your security camera, by locking your entry points, or alarming your doors, all from the convenience of your smartphone from anywhere with a network signal. As mentioned in the section on alarms, this increased connectivity between all aspects of your physical security is key, and is where much of today's innovation is focused.

📌 Night Vision

No, not magical night vision like Superman and Kryptonians. We're talking about a relatively mundane technology these days that I've already discussed in the alarms section: infrared light sensors. As mentioned, all warm bodies emit heat, and IR light is just that: Heat, or lower frequency photons. Physics notwithstanding, the upshot is that if a camera is equipped with an IR light sensor, it will be able to detect warmer bodies even when there is not visible light, which happens often—be it at night or in unlit rooms. This can be communicated to a monitor, where a human can observe it, or with modern cameras it can even be automatically processed, much like the motion sensors described above; if programmed to do so, it can send a signal to the alarm panel that there is an unexpected individual passing by the camera. This feature is particularly pertinent at night, when operators would be asleep, or in rooms where nobody is supposed to be, like a locked vault, or a server room.

📌 Durability

Switching gears a bit from IP compatibility, durability is an important factor to consider for many cameras you might wish to install. Many cameras sacrifice durability or sturdiness in favor of sleekness or aesthetic value, so if you're wishing to, for instance, install a camera outdoors, or in a place where it's susceptible to be vandalized, you will have to keep that in mind. A good choice for a more durable camera is a dome camera, simply because the fragile lens is protected by a generally polycarbonate covering, and you can even find PTZ or fisheye or multi-directional dome cameras; hey don't have to be fixed.

📌 Focal Type

Another important physical factor in a camera that you'll want to consider is the focal type. For those unfamiliar with photography, this is the term applied to the different types of lenses you can have on a camera, as your choice of focal type will directly affect the field of view of your camera. For instance, you can have a wide-angle lens, like a fisheye camera, or a prime lens, which has a fixed focal length (can't zoom or unzoom, always focuses at the same distance from the camera, useful for smaller rooms), or a zoom lens, which should be relatively self-explanatory. This is certainly an important feature to consider based on the particular topography of the area the camera will be in.

📌 Form Factor

Finally, you'll likely want to consider the form factor of a camera when choosing one. The form factor here refers to the basic aesthetics of the camera: How sleek it looks, how well it blendsor fits in with the décor, etc. If the camera is merely in a warehouse, then this won't matter as much, but if it is in a very publicly visible area, then it's certainly an important factor to consider when making the decision. Do you want to make the camera inconspicuous? Or very conspicuous, but tastefully so? Should it be garish in color to attract attention, or subdued to blend in? Questions like this are essential in the decision making process when purchasing and installing security cameras.

New Technology and the Future:

Data Analysis and AI Facial Recongnition

Moving away from commonly available features, now we'll discuss those new, cutting-edge, exciting features that will define the future of video cameras.

AI Facial Recongnition Technology

AI facial recognition might be one of the hottest topics in tech today. From controversy over Apple's new face ID method, to using Deepfakes to create hyper-realistic videos of celebrities, AI and facial rec. are at the forefront of the industry, and for better or worse, video cameras are starting to adopt it into their platform.

Now what does this represent? Well, as with the general applications of facial recognition, its uses here are varied. The most straightforward use is recognition of known/allowed persons to a space, and conversely recognition of unwanted persons. For instance, if there was a facial recognition-equipped camera at the entrance to an office, employees and authorized personnel could register their facial features so that it remembered and recognized them, and it would thus be able to detect an intruder and warn the administrator of such. In addition, if the video camera were integrated with an access control system, like Kisi, much like we discussed for alarm systems, then it could toggle the access control and unlock the relevant door when an authorized person presented their face to the camera. Similarly, when it detected an intruder or unrecognized face, it could lock the doors until actions were taken accordingly. Finally, it

Automatic Data Logging and Pattern Tracking

In another application of cutting-edge new tech and algorithms to security cameras, we have data science and analysis thrown in the mix. The general premise: You have a camera constantly recording your premises, so rather than merely using it to detect intruders, you could leverage all that footage to track employees, track use of space, and even run an audit on your office or store (this last point is less relevant for home security cameras).

First off, as mentioned with the facial recognition technology, you can use video cameras to automatically track specific employees' movements and uses of time throughout and across days. Of course, with any sort of tech like this, there are issues of privacy that will naturally come up and, while I'm not a legal expert or purporting to give legal advice, that will definitely be something to consider before putting these protocols into effect. However, that issue notwithstanding, being able to automate person tracking and systematize it has enormous potential, and there's no reason to think that it won't become an industry standard in the near future, with the massive push toward efficiency and optimization for productive time occurring today.

Similar to employee tracking, video data analysis can be used to track the use of space, and to help you optimize your allocation. For instance, if a tracking algorithm finds that too many people are using a given room too often, and it's bordering on either the unsafe or the unproductive, you can impose limitations, and reorganize desk locations, to ensure a safer and more productive environment. Following on that same safety tack, if a video system notices that at a given time the occupancy of a room poses a hazard in the case of an emergency, it can notify the administrator, who will then take steps to diffuse the situation.

Combining these points, we arrive at a natural conclusion—many offices are taking steps to run audits of their stores with video cameras. This makes sense because if you're able to gain a full understanding of all the comings and goings of people and merchandise in your store, with simple data analysis, why waste time and money on more expensive traditional methods? With these applications, video surveillance becomes one of latest industries to be revolutionized by modern data analysis tools.

Closing Thoughts

Hopefully, after reading this guide, you'll have a more clear idea of what physical security is, and what different components you might need. An overarching point throughout has been connectivity, and if we haven't stressed it enough yet, here it is again—if this guide can impart just one nugget of wisdom, it should be to integrate all your systems together. With integrated alarms, video cameras, and access control systems, you will dramatically increase the safety of your space, and ensure that you're as protected as possible.

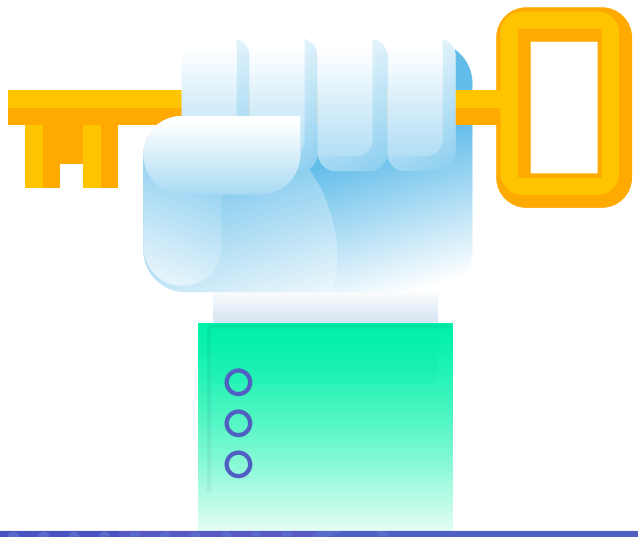
All of us at Kisi wish you the best in securing your space! Let us know how we

Contact Us

See Kisi in action

We provide an easy-to-manage system to regulate security at home or at work, and that's what you're here to discover. The best access control systems combine top-notch software (including software infrastructure, like the Cloud and IoT) with the right hardware.

How it Works



Flexible Pricing & Quotes

Get a tailored quote that fits your business location and needs with our flexible and custom rates. All paid plans come with a 30-day trial window. We also ship to anywhere in the world and install with remarkable speed.

View Pricing Plans

We would love to hear from you!

Get in touch with our sales team
Give us a brief summary of your needs and we'll get back to you within one business day

Contact Us

CALL US
+1-646-663-4880

EMAIL
sales@getkisi.com