openpath

Ultimate Guide to Access Control

What is Access Control?

Access control is a form of physical security that manages who has access to an area at any given time. Access control systems restrict access to authorized users and provide a means to keep track of who enters and leaves secured areas. It is a broad practice that includes the implementation of guards, electrified doors, turnstiles, fences and gates to keep an area secure.

In an access controlled-building, authorized persons use credentials (physical and/or digital via a mobile device) to make unlock requests at readers, which send information to an Access Control Unit (ACU), also known as an access control panel or a controller. The ACU then triggers the electrified door hardware to unlock.

The following guide will teach you everything there is to know about access control systems. Let's get started.

Access control policy considerations

When implementing an access control system, there are many factors to consider. Security should be your top concern: hardware must be tamperproof and software should be updated routinely to protect against cyberattacks. Also, look for a system that enables modern security practices like multifactor authentication, to ensure that administrative control stays in the right hands.

User experience is another important factor. Your access control system should be easy to configure for administrators, as well as accessible for employees and tenants to use.

In tandem with user experience, reliability is crucial. Look for a system with a proven track record of server uptime and a consistent unlocking experience. Vendors are constantly improving traditional access methods through biometrics, PIN codes and, more recently, smartphone credentials. However, many of these solutions are either unreliable or create too much friction. Best in class reliability calls for multiple forms of communication to authenticate an action. When Bluetooth, WiFi, and Cellular Data can be used simultaneously, the signal to unlock an entry is more reliable and the user can seamlessly enter a given space.

Another factor that is probably top of mind: Cost. Most electronic access systems range from $1,000 to $4,000 per door installed. You'll need to decide how many doors and entries you want to secure: exterior doors, interior doors, parking gates, elevators, and so on. In addition, if you are going with a cloud-based solution, you may need to pay a monthly subscription cost.

Meeting a business's compliance needs is one of the biggest considerations in choosing access control. With many different requirements, it can be difficult to track which standards are most important. Here are some requirements you may be asked to meet:

- **PCI** - Requirements 9 and 10 are common areas to address in physical and network security. Requirement 9 mandates organizations to restrict physical access to a building for onsite personnel, visitors and media. The business should have adequate controls to ensure that no malicious

individuals can steal sensitive data. Requirement 10 relates to the need to track and monitor systems.

- **HIPAA** - Although most think of this requirement within the healthcare context, employers also deal with a large amount of health information. For instance, when an employee requests medical leave, employers need to keep any documentation of that absence confidential. In order to meet this requirement, businesses can use access control to keep this information locked in a storage room.

- **SOC 2** - This auditing procedure enforces service providers to manage data to protect employee and client privacy. Companies in the SaaS space are eligible to receive SOC 2 certification by purchasing an access control system with two-factor authentication and data encryption. Any business dealing with customer data must protect PII (personally identifiable information) from unauthorized access.

- **ISO 27001** - This information security standard requires that management systematically examines an organization's security risks and audits all threats and vulnerabilities. It also requires a comprehensive set of risk avoidance or transfer protocols and have an overarching management process to ensure that information security continues to meet the business's needs on an ongoing basis.

- **MPAA** - Organizations dealing with content, such as video and audio, seek security protocols to prevent pirating, theft and other types of breaches. Although the MPAA doesn't mandate compliance, sticking to this best practice helps members ensure content protection during production, post-production and distribution. Access control can help manage entry and exit points in addition to logging, monitoring and a variety of other systems.

- **CJIS** - In 1992, the FBI created this organization to monitor criminal activities through analytics and statistics. Today, the organization has a few best practices related to security and authentication. From an access control perspective, this includes restricting access based on physical location or time of day.

Effective physical security practices require being proactive. By taking on these considerations, you can develop a basic framework for your company's access control needs to maximize security and ROI.

Understanding access control models

Access control models originated as network security concepts (i.e. controlling access to files on a network rather than entries in a building) but are sometimes used in the context of physical security. The three most common models are:

- **Discretionary access control (DAC)** - The business owner decides which people have rights to a specific area in a building through some type of control panel. It is the least restrictive model because business owners are not security experts and may inadvertently provide the wrong level of access to an individual. Therefore, this model is seen as risky to a business so it is used the least.

- **Mandatory access control (MAC**) - This model is often used in organizations that require a high amount of confidentiality. MAC utilizes a central authority to classify the access given to each employee through established guidelines. Large organizations, specifically in tech, may find MAC to be suitable for their company by having a Chief Security Officer in headquarters responsible for determining policy across many different locations. MAC enables companies to have consistent access control practices in-place without compromising best practices.

- **Role based access control (RBAC)** - Most of today's businesses deploy this model to segment access based on job titles. The system administrator will use practices such as "least privilege" and "separation of privilege," to ensure each role only receives access to the areas they need. Role-based access may incorporate rules such as when a group can enter the building. Some advanced access control vendors allow administrators to create rules for guests using a mobile device. Although RBAC might seem complex, it is relatively easy to implement and the most secure.

Key components of access control

In an access controlled building, authorized persons use credentials to make unlock requests at readers mounted proximate to entries, which send information to an Access Control Unit (ACU) that makes access control decisions that triggers electrified door locking hardware.

Credentials: There are several types of credentials available to businesses in today's physical security environment. Below are the most popular methods of credential available.

- **Key cards and fobs** - These tend to be popular choices for access control because they're relatively cheap and are more user-friendly traditional metal keys. There are several different kinds of card and fob technologies, but the most common are RFID cards/fobs and swipe cards. RFID stands for Radio-frequency Identification. RFID key cards come in a variety of formats and protocols, but the two main types are:

    - **Proximity cards** - These cards communicate using low frequency fields (typically 125 hHz). These cards typically use the Wiegand protocol and have a short read range of 1-10 cm.

    - **Contactless smart cards** - These cards contain a smart card microchip and communicate using high frequency fields (13.56 MHz). The standard protocol for these cards is ISO/IEC 14443 and the read range is one centimeter to one meter.

  Swipe cards (also known as magstripe cards) use the same technology as credit cards: a magnetic stripe stores data, which is read by a swipe card reader. The kinds of swipe cards used in access control are high-coercivity (HiCo) meaning they require more magnetic energy to encode which makes them harder to erase and therefore more secure and reliable than low-coercivity (LoCo) cards. However, swipe cards are still considered less secure than RFID cards because they're usually not encrypted and are easy to clone.

Key cards and fobs are cheaper and easier to manage than traditional metal keys, but aren't always the most secure or reliable – whether because they're easily lost, cloned, or because they wear out quickly. Here are a few reasons why they are far from an optimal solution:

- **Easily lost or stolen** - It's not uncommon for employees to forget or misplace their key cards on a regular basis. In addition, visitors can inadvertently forget to return cards, creating a security risk.

- **Not always secure** - Not all key cards are the same – some cards, like MIFARE, are designed to prevent key cloning. Other cards that use the Wiegand protocol are more vulnerable to sniffing and copying.

- **Cumbersome to use** - With all the convenience RFID technology provides over traditional keys, it still requires a user to fish their key card or fob out of their pocket/bag to present to a reader.

- **Not reliable** - The magnetic stripe wears down after regular use, so you need to replace cards more often.

- **PIN code** - A PIN reader, as its name implies, uses PIN codes instead of physical credentials to grant access. Depending on the model, a PIN reader might operate as standalone and only accept one master PIN code, or it may connect to an access control system where users have individual PIN codes that determine which entries they have access to and during which times. The problem with PIN codes is that they're both easily forgotten and easily shared, meaning they're not ideal for areas that require high security.

- **Biometrics** - In access control, credentials can be categorized as something you have (a key card), something you know (a PIN code), or something you are. Biometric credentials fall under that last category; they include data like fingerprints, palm veins, and retinas. Biometric reader pricing ranges from low end (a fingerprint scanner) to high end (multi-input readers).

- **Mobile** - Mobile credentials let you use your smartphone to unlock entries. In the access control administrative software, a user is assigned a mobile credential. The user installs the access control mobile app on their smartphone, logs in, and approaches a reader. The user then makes an unlock request using their smartphone —either by tapping a button in the app, holding up the phone to the reader, or by simply touching the reader with their hand while their phone is in their pocket or bag. This request is sent to the ACU through the reader via Bluetooth, or directly to the ACU via Wi-Fi or cellular data. Once the mobile credential is authenticated and authorized, the entry unlocks.

- **Readers:** Readers are devices installed near entries that receive inputs from user credentials via radio frequency signal (RFID, NFC, or BLE) which they then relay over a wired or wireless connection to ACUs installed nearby.

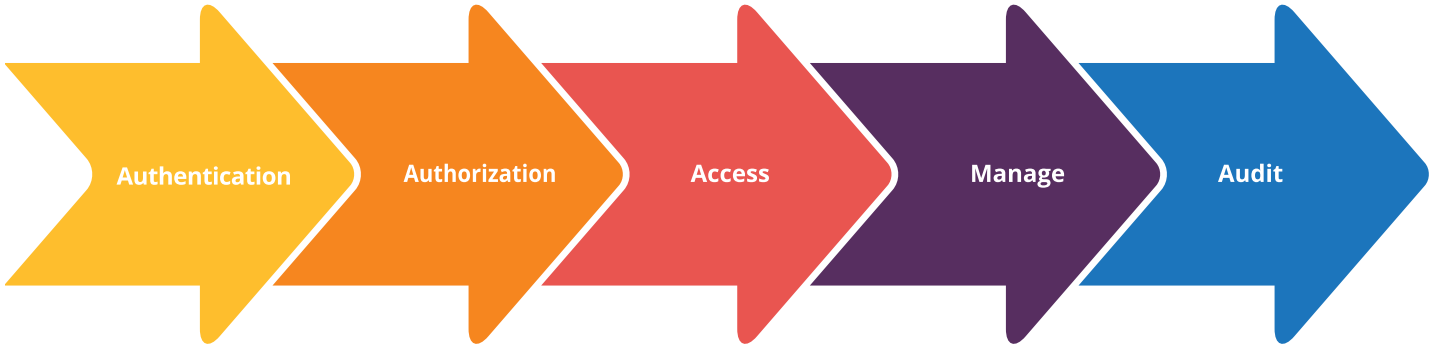
- **Entries:** Entries include any electrified or automated opening: doors, parking gates, turnstiles, elevator floors, storage cabinets — anywhere where access needs to be restricted Door contact sensors indicate whether a door is open or closed, propped or forced open. Request to Exit (REX) sensors and buttons are used to unlock doors automatically when someone exits an entry.

- **Locking hardware:** Door entries are configured with electric strikes or electromagnetic locks.

- **ACUs:** Readers send credential data to an ACU (also known as a controller or a control panel), which decides if a user has access or not. If they have access, the ACU then instructs the door locking hardware to unlock. One ACU usually supports between 2 and 8 readers.

- **Software:** All of this hardware is managed with access control software — an application where you define users, credentials, access schedules, entries, and so on. The information defined in the access control software syncs with the ACU, which is how it knows whether to grant or reject access. Cloud based software systems are the most open approach for access control solutions.

How access control works



1. Authentication - First, a credential is authenticated. After a user presents a credential (mobile credential or car/key fob) at a reader, that credential's data is sent to the Access Control Unit (ACU), where the ACU determines if this credential is known and recognized by the system. If a credential has been added to the system during an Internet outage, the ACU will not recognize the credential until the Internet is restored.

2. Authorization - Next, the ACU determines if the user to which this valid credential belongs is authorized for access – does the user have access to this particular entry? Are they using the right kind of credential and trigger type for this entry? Are they attempting to unlock the entry within any applicable schedules? In order to be authorized, a user must:

- Have access to the entry they're trying to unlock
- Use one of the predefined allowed credential types (for example, mobile credential)
- Use one of the predefined allowed trigger types (for example, onsite 2FA)
- Make the unlock request within any schedules defined on the entry or assigned to the user or their group

3. Access - Once authenticated and authorized, the ACU then sends a command to the door locking hardware to unlock the entry. In the case of electromagnetic locks, power is temporarily interrupted when unlocked (also known as fail safe) whereas with door strikes power is temporarily applied to unlock the door (also known as fail secure).

4. **Manage** - Managing an access control system includes adding or removing entries, users, credentials, schedules, and alerts using administrative software that syncs automatically with Internet-connected ACUs. The newer cloud based access control systems integrate with directory services like Google G Suite and Azure Active Directory, streamlining the management process. They also provide the most flexibility for service enhancements versus legacy systems which are client-server based.

5. **Audit** - Administrators can audit access control systems by generating reports for access logs, including both user activity and entry activity. This is useful for general system reviews; ensuring that the system is working as expected and that there are no issues with accessing entries. Reports are also helpful for meeting compliance standards, such as HIPAA, that require a certain level of physical access control. Additional audit capabilities are provided by access control systems that integrate with Visitor Management Systems, Video Management Systems (VMS), and other security type platforms.

Access control hosting options

When purchasing access control systems, it's important to look at the benefits and drawbacks with each type of system. One of the biggest decisions you'll have to make is whether or not you want a solution to be on-prem, web-based or in the cloud.

Here's an overview of the types of hosting options available:

- **Server-based** - Traditional access control solutions use dedicated servers onsite that communicate with ACUs and readers over a LAN connection. In the case of multiple buildings or sites, separate servers and software must be purchased, installed, and maintained at each location in order for the system to operate.

- **Embedded (aka web-based)** - Browser-based access control systems operate similarly to dedicated server systems but also include a web application. Internet access is not required for the application to work; the application connects to the LAN and can be accessed on any device within that network.

  Embedded systems are similar to server-based systems but they differ in that the access control software is preloaded on the access control unit itself, and then accessed via a web browser. Like a server-based system, everything communicates over a LAN, so an Internet connection is not required.

There are also several costs related to hosting the software. Here are a few examples:

- **PCs/servers to host the access control software** - In legacy access control systems, dedicated hardware is required in order to run and manage the access control system. This hardware must be purchased and then maintained throughout the life of the access control system. This also requires more room in the server closet.

- **Additional workstations to manage the access control system -** In addition to the access control server, workstations are often used to make maintaining the system more flexible and remote-friendly. The cost of hardware for additional workstations is especially an issue for large, multi-building sites.

- **Administrative software licenses** - Software that is installed on dedicated servers and workstations often requires individual licenses to operate. Also, major software upgrades might come with additional costs, including any IT resources needed to perform the upgrade.

- **Key cards/fobs** - Key cards and fobs might seem like a small expense, but the upfront cost of providing credentials to employees and tenants is a factor to consider. Also, the cost of replacing lost and stolen credentials can add up quickly.

- **Ongoing maintenance and upgrade costs** - Often, legacy access control systems are maintained by dedicated IT resources, which can be expensive.

There are several additional challenges associated with legacy access control systems. First, they are high maintenance.The main difference between legacy systems and cloud-based systems is that in legacy systems, the software resides on hardware maintained by the end user offline. In cloud-based systems, it resides in the cloud (i.e. on a remote system of servers) maintained by a third party.

Another problem is that legacy systems can't be managed remotely. Since the access control software can only be accessed over a LAN, administrators must use in-network devices to make changes to the system, making it difficult to manage remotely. In addition, they typically use outdated security methods, and they're limited in the types of credentials they support: PIN pads, key cards, and fobs.

- **Cloud-based** - Cloud-based access control runs the access control software in the cloud (i.e. on a remote server) that regularly syncs with the local ACUs. Because the software is cloud-based, administrators can easily add new users or revoke access using any web-enabled device, and the ACU is updated automatically. This type of access control system requires internet access, but can

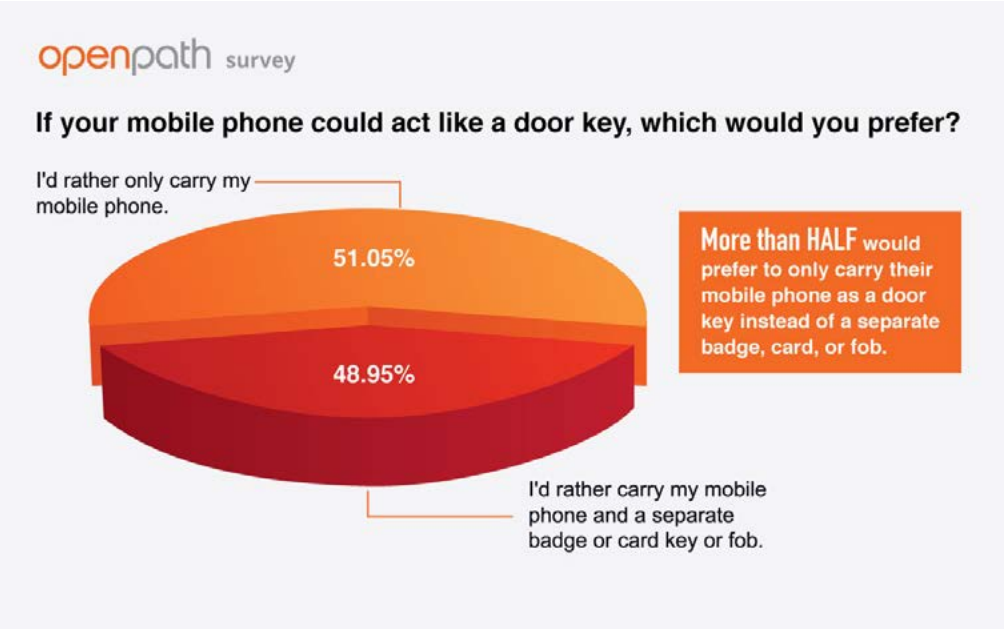
still function without it — any updates made using the software will take effect after Internet access is restored.

In a cloud-based access control system, the hardware is installed on site and configured using the cloud software. Users, entries, schedules, and site information are set up in the software and then automatically synced with the ACUs. Similarly, unlock requests and entry status changes are reported to the cloud software in real time. In the case of power and Internet outages, the system will still function but communications between the software and the ACUs will only take place once power and Internet are restored.

There are several benefits that come with implementing a modern, cloud-based access control system:

- **Increased security with reduced overhead** - A modern access control system keeps unauthorized persons out while also making it easy to revoke access or remotely lock entries at any time. Modern systems are easier to install, configure and manage, reducing the need for ongoing, costly IT resources. In a mobile-enabled system, administrative overhead is reduced as you don't need to print, issue, collect, and track physical badges, fobs, and keycards (but can still utilize in conjunction with a mobile credential capability if preferred by certain users).

- **Better accessibility** - Instead of traditional locks and keys or access cards (that are easily lost or cloned), mobile credentials offer an easier, more secure way to enter access-controlled spaces. Guest access links let you easily provide access to visitors via email or SMS, and remote unlock capabilities mean you can unlock entries from anywhere. Plus, cloud-based access control is ideal for providing access across multiple buildings and sites because it's designed to scale with your needs.



- **Seamless integrations with smart office technology** - Modern cloud-based access control systems are designed to work with the latest technologies – make the most of your access control by integrating with HVAC, lighting, alarm systems, as well as directory services (like Azure Active Directory, G Suite, and Okta) and messaging platforms like Slack. Compare this to traditional access control systems which are often proprietary and only offer a few select native integrations.

- **Future-proofed** - cloud-based systems provide the greatest combination of security, flexibility, speed and reliability, and new enhancements delivered in real-time.

Applications for access control

Access control systems have long been treated like commodities —for good reason. They are the front line in securing any business's door or entrance. As a result, there are several industries that can benefit from a secure access control solution.

Here are some of the most common applications for access control across industries.

- **Commercial real estate** - As offices evolve to accommodate more flexible working conditions, businesses need to provide next-generation security with fast and reliable access control. In addition, it needs to have an open API that can connect to modern apps such as Slack and other office support systems, such as guest management, and video, to provide a truly user-friendly interface. The right solution can increase worker satisfaction, reliably keep employees safe and effectively manage various risks.

- **Multi-store retail** - Would you give away free products? Without the right system in place, you may be doing just that. Shrink, whether it's from employees or shoplifters can play a significant role on a company's bottom line. An employee-friendly access control system helps staff get in and out of the store as needed without fumbling around for a badge. Given high turnover rates in the retail industry, smart access control allows employees to be added and removed from the access control directory when they are deleted from other management systems allowing for necessary scheduling and credential changes without extra labor.

- **Multi-tenant housing** - For years, security protocol in multi-tenant housing meant having a door buzzer on a lobby entrance with an intercom. Upscale buildings often augmented this with doormen who checked in any visitor that enters to ensure only authorized guests are permitted. However, with rising rents in metropolitan areas, landlords need to think strategically on how to lower their costs while adding value. Adding a state-of-the-art access control solution accomplishes just that. Through the installation of a mobile access system, landlords can give tenants an easier way to access common spaces such as mailrooms, garages and gyms. In addition, access control can be used as a marketing tool by empowering tenants with the ability to grant mobile guest passes to delivery services, dog walkers and postal workers.

- **Education** - Whether you're in a K-12 setting or a university, protecting students and teachers is a top priority. As violence becomes more prevalent on school campuses, school administrators need to ensure that students feel safe in their learning environments. With mobile credentials, schools can create a welcoming environment that will ensure student safety by making sure only those who are students and faculty have access to a campus. On top of the different security demands including lockdown capabilities, public schools often need to meet a certain attendance quota for tax purposes. By looking for an access control solution with an open API, administrators can actually turn security into a profit center by integrating the system with their time and attendance software. This helps schools increase funding, therefore improving the education for students.

- **Religious institutions** - Unfortunately, religious institutions are vulnerable to vandalism, burglary and violence. However, they also want to project a welcoming atmosphere and openness to all of their congregants. This can create a significant challenge: a security gap can make the institution vulnerable to attacks, while too much protection can appear intrusive. A state-of-the-art access control solution can solve this problem by blending into its physical surroundings, supporting multiple access methods to foster accessibility, and having a strong lockdown capability. Outside of the service itself, a religious institution often needs to provide access to temporary visitors such as volunteers or parents. With a flexible access control solution, clergy can focus more on serving their community instead of worrying about their safety.

- **Healthcare** - Access control in the healthcare industry requires an innovative approach that requires the ability to access main and internal entrances. In addition, any access control solution must possess data that integrates with various rules, such as shift changes or specific department access. In addition, healthcare facilities rely on access control to ensure narcotics, substances and medical records can only be reached by authorized users.

- **Government** - In 2004, then-President George W. Bush ordered the sweeping Homeland Security Presidential Directive-12, which states that all access control systems must be upgraded to include Personal Identification Verification credentials in accordance with the National Institute of Standards and Technology guidelines. Given the risks facing government facilities such as access to sensitive areas, crisis management and unauthorized facility access, working on the national level requires meeting several security standards. The local level has lower certification standards, providing elected officials with more flexibility in choosing an access control provider.

- **Sporting and entertainment events** - Sports leagues and musicians alike are providing more access to fans than ever before. But how much access is too much? Arenas pose a unique challenge for several reasons. Stadiums can hold tens of thousands of people, making the arena itself particularly vulnerable to acts of mass violence In addition, athletes, media and vendors all require access to different rooms, each with distinct security requirements. With the right access control solution in-place, security teams can create a nuanced policy that is inviting for fans, but doesn't sacrifice safety.

- **Data centers** - Many businesses store servers in a room dedicated to the continuous operation of a company's network. Unlike an office, this area is exclusively accessed by IT staff. However, like the modern office, IT positions are becoming more flexible with the rise of remote work. As a result, businesses are forced to accommodate the needs of today's employees. As a result, IT departments require a versatile solution that is easy to manage remotely Given the sensitivity of many data centers, it's crucial to have reliable access to these rooms with a system that is indestructible from a security perspective.

- **Oil and gas** - Given the volatility of oil prices, a breached refinery could cause an international crisis. Therefore, it is crucial for sites to be closely monitored at all times. While most sites already have video surveillance, many refineries are utilizing access control to reduce the number of operators needed at a given site. In particular, the integration of access control to video surveillance enables license plate recognition technology to ensure that only authorized vehicles are entering the site. Through an intelligent system, the reader could check a license plate against a database and grant access to the required areas.

- **Hospitality** - As companies like AirBnB and Homeaway disrupt the hospitality industry, hotels are under increased pressure to make their hotels amenable to guests while maintaining a high level of security. As a result, they are adding amenities such as concerts, shops, full bars and more all within the confines of a hotel. With each addition comes additional security vulnerabilities. A mobile access solution can help mitigate the challenges of having multiple

vendors through easy-to-use credentialing and guest passes that can be transferred via text message. In addition, hotel managers can assign each vendor specific access privilege so they can spend more time building their customer relationships.

- **Transportation** - Public transportation stations pose several security challenges as they deal with a large number of people and constantly changing traffic patterns. In addition, the stations are typically small and sit outside the secured area of public transit. This often leaves employees and critical assets exposed to many security threats, which can ultimately impact public safety. An IoT-enabled access control system improves employee safety in the station's office without the annoyance of needing a key or badge. In addition, it can play a valuable role in time and attendance by tracking when the employee arrives so managers have an accurate record at all times, and know who is where in case of any safety/security issues.

- **Airports and seaports** - Airports have both hard and soft targets, creating unique safety challenges. While TSA focuses mainly on securing the terminals to prevent criminal activity in an aircraft, there are a number of vulnerabilities around the airport as well. Vehicle entry points at the perimeter are often unmanned. As a result, restricted access areas can become surprisingly vulnerable without an access control solution that is both secure and employee friendly. Seaports face similar challenges as a large open venue that is have to maintain compliant according to ISPS standards. This means that any companies with business on a port must meet strict security measures. An innovative access control system helps manage all employees and vehicles to ensure proper access to that port.

- **Banking** - Financial institutions are constantly under attack. Banks are vulnerable to a host of threats including robbery, fraud and terrorism. However, brick-and-mortar banks are beginning to cut back on the number of tellers and staff as a majority of consumers opt to bank on a mobile app or online. This leaves branches with increased pressure to secure storage rooms, back offices and other areas that are susceptible to breaches. Instead of using easy-to-hack keypads, an IoT access control system can lock storage closets and offices without the presence of a physical guard. Banks need the capability to easily manage the security at each branch without requiring the physical presence of an officer.

- **Warehousing** - Today's warehouses are becoming smarter and more automated than ever before. However, the security outside the warehouse often lags behind from a technological perspective. Many companies are still using traditional locks or key pads to get into the room. The problem is that a lost key can create a significant expense and key codes are easy to share with other employees. Through a smart access control system, warehouses can ensure their inventory is safe at all times - and even work with a robot to ensure a safe, efficient operation.

- **Gaming** - Casinos rely on strict physical security in order to keep cash and chips safe. Most rely on key management systems to track access to different safes and drawers. For some casinos, this means storing hundreds of keys, all of which require a tiresome amount of accountability and reporting to ensure employee honesty. Thanks to modern access control, this process is no longer necessary for casinos. In fact, with the right strategy, chips and cash can be better managed through mobile access.

Criteria for selecting an access control system

Selecting the right access control system can be an exhaustive task. After all, there are hundreds of solutions on the market, all with distinct features. Determining the right solution will depend on a variety of factors such as the size of your business, budget, the number of readers you need, and your building's business objectives.

Whether you're working with a systems integrator, architect or researching on your own, there are a number of questions you can ask to ensure that the system you are implementing is right for you:

- **How reliable is your access control system?**
  Electronic access control systems rely on various technology such as biometrics, Wi-Fi, NFC and Bluetooth. The problem is that these technologies require 24/7 uptime or some type of accurate reading in order for the system to work. However, reasons such as misread fingerprints, acts of god or random internet outages can cause the system to fail. As a result, most access control systems have at least some reliability issues, creating a poor user experience.

- **Does the access control system integrate with existing security infrastructure?**
  Most buildings have some type of video surveillance in place to ensure employee safety and protect the business from theft. However, with the advent of video management systems (VMS), organizations can now perform more complex functions such as people counting, license plate recognition and even predict incidents before they happen. Having an access control system that integrates with your VMS enables businesses to operate their security operations more efficiently and collect more data. In addition, they can connect with other systems such as guest management systems and alarm systems.

- **How does your system work with intrusion detection?**
  Many of the newer access control companies have the ability to integrate intrusion detection technology into their system. Intrusion detection allows companies to lock, unlock doors and rearm

the doors all at once by using some type of credential such as a card, fob or even mobile device. This functionality prevents an employee from needing to lock every door in the office and setting an alarm before he or she leaves for the day.

- **Can this system integrate with existing office automation functions?**
  Some access control systems have added intelligent automation to integrate seamlessly with various business apps and even devices. Adding this level of functionality enables businesses to use their access control system creatively for functions such as visitor management, lighting and room booking. As IoT-enabled devices shift from disrupting the home to the office, it will be important to look for solutions that can enable complete office automation.

- **Will my employees be able to easily use this system?**
  While your employees are likely to welcome using their smartphones opposed to the burden of remembering a fob or key card, some technological upgrades will create added friction. For instance, many of today's mobile access control systems require the user to unlock their phone before using. Since this adds extra steps, users might simply prefer a more intuitive key card than smartphone credential technology In addition, biometrics solutions require the user to have a clean fingerprint or line up their eyes directly with the reader. As a result, this can delay users by several seconds and create frustration. The ideal access control solution is one that doesn't require the app to be open, and/or the phone to be placed over the reader.

- **How will a modern access control solution evolve with my business?**
  The modern office is constantly changing to adapt to the flexible worker. As millennials are now the single largest segment of today's workforce, and an even more technologically savvy Generation Z enters the workforce, employers can attract talent by implementing access control technology that allows employees to work flexible hours. In addition, companies need a solution that can work with various apps they are already using at work. In order to make these accommodations, businesses should invest in an access control system that has open APIs, is based on the cloud and integrates with the rest of the office. As the Internet of Things increases in popularity businesses should seek applications that maximize technology and are customizable to their employees' needs.

- **What security features does your access control system have?**
  Problems such as cloning, lost/stolen access cards and reader vandalism are common problems in the access control industry. Any one of these problems can have a detrimental impact on your company's security. Leading access control companies are utilizing multi-factor authentication to provide clients with an added layer of protection. This helps ensure that the user trying to unlock the door is truly who they say they are. In addition, your access control solution should have a back-end system that enables real-time monitoring to determine each instance of failed entries, ajar notifications and any

other irregularities that occur at your office. Time based entry is another feature enabled by cloud-based access control.

- **How does your solution work with controlling elevator and garage access?**
  In order to add an extra layer of security, buildings are starting to deploy access control systems in elevators and garages. In fact, several corporate offices now have smart "destination dispatch" elevators, which allow passengers to request a particular floor using a touchscreen or keypad. This ensures maximum efficiency and prevents overcrowding the elevator. As part of the added intelligence, elevators are also checking to make sure each individual has access to their respective floors. Garages, especially in urban communities are vulnerable to criminal activity without proper access control in place. If either of these requirements are important, ask your prospective vendor about if this functionality is available and figure out what sort of manual labor is involved.

- **Can your system handle inclement weather?**
  Surprisingly, durability is not a key feature with many access control solutions. This can at times make readers malfunction in cold environments, rain or dust. You can ask your integrator if this system has an IP65 rating if you're planning to install your reader outside.

- **What sort of mustering scenarios does your system handle?**
  Mustering is a powerful feature in the access control industry that allows admins to use access logs to locate people in a building or specific area. This capability analyzes the logs to determine where a user is in the facility and can help with time and attendance tracking. A mustering system can use time logging to track a user's movement throughout the building by providing insights into where a user was at a given time. This is often valuable when a building administrator needs to track potential criminal activity or for safety needs.

Conclusion

The need for top-notch security has never been greater. In a post 9/11 world where physical security threats continue to grow, offices and schools need to take the safety of their employees seriously. Simultaneously, employees are increasing their own expectations of their employers to eliminate friction in the workplace, such as accommodating flexible work schedules.

These requirements mean companies need to pay more attention to finding security solutions that address both the needs of administrators and their employees. Thanks to advances in access control technology, especially cloud-based solutions, it's never been easier to meet these challenges.

Ready to learn how Openpath can help you and employees enjoy both convenience and security?
Contact us or call 844-673-6728.

About Openpath

Our story started when we noticed how much was missing from the keyless entry experience. What was out there didn't work well, didn't look good, and was overpriced. The moment we went all-in on creating a new standard for the industry, we knew we were on to something big.

History

Openpath was created by a team of serial entrepreneurs who were tired of forgetting their office keys at home, frustrated with having to carry multiple badges to get into their buildings, and seriously worried about the security of their workspace given the state of the world today.

We've worked extremely hard to build a company that can offer a new, seamless style of security that takes advantage of new technologies, and makes people feel safe at work. Access Control is the flagship product in our mission to improve the quality and safety of the modern workspace through automation.

Mission

Reduce friction in the modern workplace.

For the office that doesn't want to compromise ease for security, Openpath is innovative, intelligent access control that automates your security infrastructure, so you can focus on managing your business.

Contact us or call 844-673-6728 for more information.