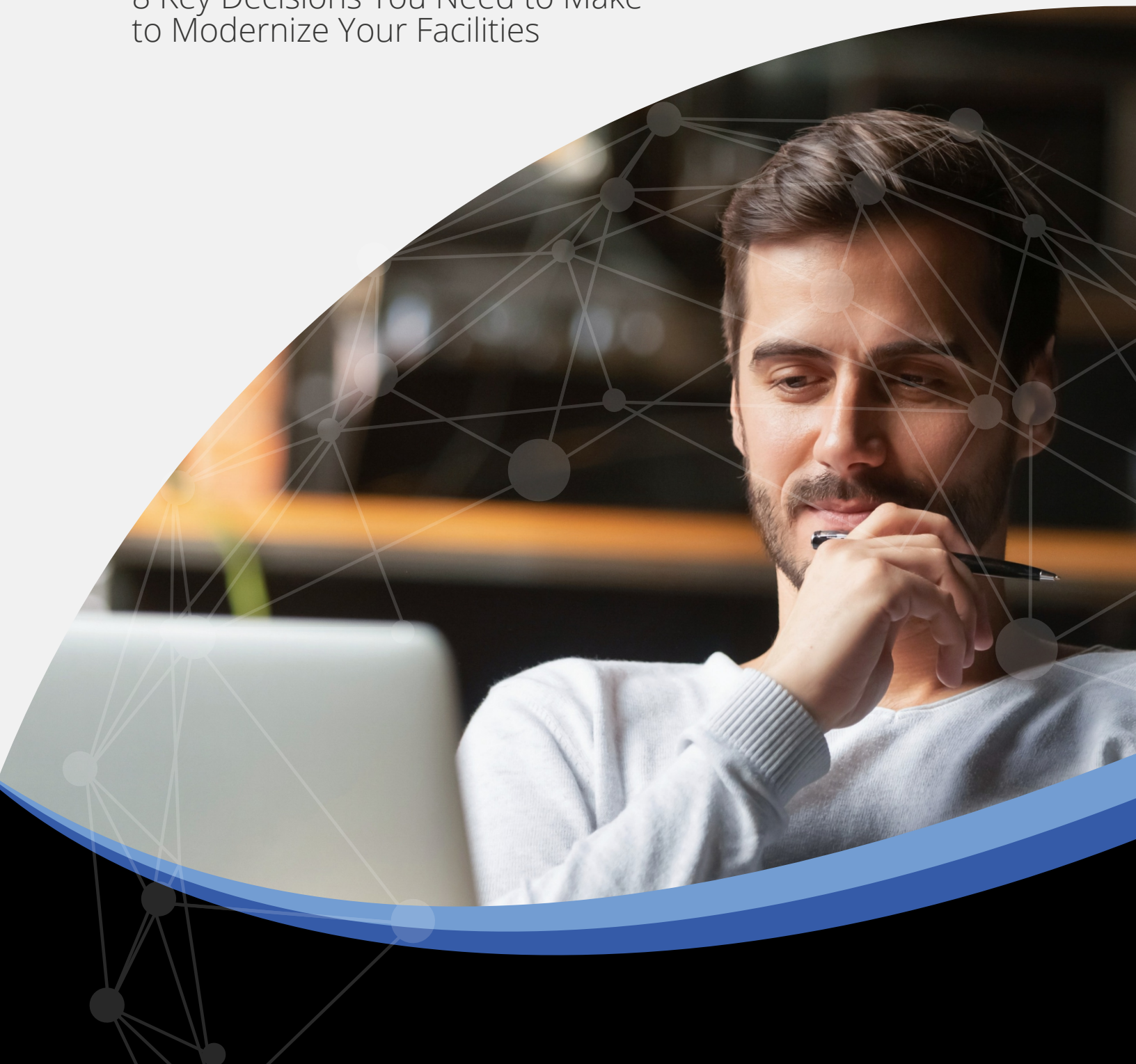
brivo

Access Control: The Enterprise Buyer's Guide

8 Key Decisions You Need to Make to Modernize Your Facilities



Content Index

ENTERPRISE SECURITY CHALLENGES

Enterprises today face steep security challenges. They must keep their facilities safe and protect their employees. Safeguarding assets is essential and must be done in a way that is consistent with corporate policies and risk profile. And there's no single solution to this complex equation. Most enterprises harness a range of systems, devices, and applications that they must then integrate with other applications and processes. Designing a system that embraces a sophisticated, multi-layered security approach is paramount. Where should you begin?

KEY PRINCIPLES FOR ACCESS CONTROL

Smart technology and inexpensive components have turbocharged access control systems. But a successful access control solution is more than the sum of its parts. Consider these key principles when choosing and designing access control:

- **Security |** Different areas may have different access control requirements
- **Integration |** Connecting systems improves workflow and investigations
- **Scalability |** The platform you select should scale to meet growth and changes
- **Requirements |** Systems should adhere to state, local, federal, and international regulations. (e.g., General Data Protection Regulation)
- **Optics |** Effective access control sends a strong message, lets staff, clients, and visitors know you care about their safety and lets adversaries know that they should look elsewhere

SECURITY VARIES BY INDUSTRY

Different industries and sectors need different security systems. Why? Here's a partial list of the dimensions to consider:

- Nature of staff
- Type of clients
- Resource-sharing agreements
- Assets that need protection
- Bandwidth availability
- Industry regulations
- Building codes
- Contracts
- Environmental conditions
- Physical location

For example, mining operations need systems that work in harsh environments with low bandwidth. Defense contractors focus on systems that follow national industrial security regulations. A local medical practice needs two to three doors secured electronically. A large medical center with high traffic needs to protect staff, patients, and facilities with access control that includes mobile credentials and video monitoring. Suitable access control systems cover a wide range. In some cases, a single keypad will suffice. In other cases, an enterprise might need a multi-layered network spanning campuses and technologies.

THE 8 TOP CHOICES YOU NEED TO MAKE IN YOUR ACCESS CONTROL SYSTEM

1 On-premise or Cloud-based?

Businesses face two choices for hosting access control systems: on-premise or deploying cloud-based solutions. On-premise systems rely on servers hosted at the organization's physical site. In contrast, cloud-based systems rely on remote servers maintained by expert providers. Cloud-based systems do use some on-site hardware like card readers and access panels. As the name suggests, cloud-based systems handle essential functions like processing and storage off-site - in the cloud.

When considering an access control solution, either on-premise or cloud-based, security professionals must examine upfront and ongoing costs. These could cover hardware, software, maintenance, power consumption, dedicated floor space, and staffing for on-premise solutions. Planning efforts must multiply these costs by the number of business locations. (Each location needs a local server with licensed software and staff to support it.) The other dynamic to plan for is data access. On-premises systems do not enable remote network access. Authorized personnel can only access data when they are present on-site.

Cloud-based systems offer flexibility in cost and access. Cloud providers offer monthly or annual subscriptions to manage systems on your behalf, saving you upfront costs and day-to-day staffing management. Lower monthly payments replace upfront investments in hardware. This model also lowers maintenance costs. It eliminates the need for servers at each location along with support staff to manage them. Authorized staff can be centrally located and can access the system remotely.

ON-PREMISE | PROS:

- System is fully customizable to fit specific requirements
- Some government contracts mandate this level of system control

ON-PREMISE | CONS:

- Servers cannot be accessed or managed remotely, access changes must occur on site
- Requires physical access to your server and network, requiring IT staff assistance
- Requires dedicated space, cooling, and power for servers
- Requires constant manual data backups and firmware updates
- Limited in scalability and flexibility
- Multiple sites require multiple servers
- More susceptible to data loss during disaster situations
- Up front, on-site licenses can be much more expensive than cloud licenses

CLOUD-BASED | PROS:

- Lower up-front costs
- Unlimited scalability: components and users can be added or revoked at any time
- Connect and control from anywhere and any device
- Data, software, and backups update automatically
- Upgrades, virus and malware protection, and other updates occur automatically without service downtime
- Eliminates risk of lost or stolen keys/keycards
- Leverages expertise of vendor's security resources

CLOUD-BASED | CONS:

- Service policies may limit what customers can do with their deployments
- Migrating services from one vendor to another may create hassles
- Monthly pay-as-you-go subscriptions could require certain enterprises to change their approach to budgeting

ADDITIONAL CONSIDERATIONS:

Future-proof – How easy is it to add capabilities without costly infrastructure changes that grow with changing needs?

Time saving – How fast can you deploy and scale the solution?

Total cost of ownership – Beyond the hard costs of deployment, what ongoing and tertiary costs will be incurred.

2 Wired vs. Wireless Locks?

Businesses have two choices when connecting access control locking hardware. Traditionally, security systems have relied on cables to deliver data and/or power to hardware. In large facilities, cable-wired systems need specialists to thread conduit over expansive areas. Wiring must be hidden for security and safety, i.e., posing a tripping threat. And this can get complicated. For example, it could entail going through walls, ceilings, or other spaces, laying cable, and then making cosmetic repairs.

Wireless connections to access control devices are the alternative. While they have a shorter read-range than wired systems, they do not require expensive, invasive cabling. In general, modern wireless systems are on par with their wired counterparts. Wireless installations are always quicker and easier. When cable is cost-prohibitive or might damage a historic structure, wireless is a great alternative.

WIRED | PROS:

- Reliable, uninterrupted connection
- Offers more control over when connecting devices to the network
- Faster signal speed and less interference
- More cost-effective or workable for remote applications

WIRED | CONS:

- Cost of running cables and installing access panels or power supplies
- Not feasible for certain building materials like marble floors or cinder block walls
- Troubleshooting problems can be difficult and time consuming
- Upgrading existing structures can be burdensome and expensive

ADDITIONAL CONSIDERATIONS:

Labor savings – hardwiring takes longer than wireless, requires more planning. and several visits to install

Connectivity – wireless traffic is susceptible to interference and power failures, so ensuring back-up and local storage are available to stay operational

3 Legacy Readers or Smart Readers?

Access control readers are common sights at doors, turnstiles, and gates. Legacy readers are usually proximity-based, low-frequency (125KHZ) readers that communicate with physical proximity tokens such as a card or fob. They furnish one-way communication to gain entry. While legacy readers are relatively inexpensive, they pose security challenges. For as low as $15 on Amazon, anyone can buy a proxy card reader and duplicator used to create fraudulent credentials and gain access. These readers don't support encrypted credentials or mobile credentials using the latest Bluetooth and NFC technology.

Smart readers are more secure, versatile, and streamlined. They accommodate a range of access methods like high-frequency encrypted smart cards and fob credentials, as well as biometric and mobile credentials. They also offer data encryption and mutual authentication. Smart readers can communicate over the OSDP protocol for a more secure connection to the access control system.

LEGACY READERS | PROS:

- Already be in place in some facilities and can work with access control systems
- May cost less than Smart Readers

LEGACY READERS | CONS:

- Communicate over a less secure protocol
- Focused on proximity-based low-frequency credentials, which are easily duplicated
- Not compatible with new mobile credential technology such as Bluetooth or NFC

SMART READERS | PROS:

- Supports higher security level of credential technologies
- Encrypted data storage and communication meet the highest security requirements
- Scalable for small or large deployments
- Supports lockdowns
- Flexible integration
- Activity monitoring with real-time updates

SMART READERS | CONS:

- Potentially cost more than legacy readers

ADDITIONAL CONSIDERATIONS:

Future-proof – new smart readers compatible with modern credential technology

Total cost of ownership – For access control modernization, you may wish to repurpose existing readers, even if lower quality, as to not have major upfront cost. You need an ACS that can work with multiple reader types vs. proprietary walled-garden systems

4 Physical Credentials or Modern Mobile & Biometric Credentials?

Legacy physical credentials still dominate access control. The most common are proximity cards, fobs, and some legacy magnetic stripe cards. There are nuances for each type but in general, users must take physical action to gain access. Users swipe, tap, insert, or stand within a specified physical range of a reader to gain access. There are great differences in the security of each type of credential.

Modern forms of credentials are growing at a faster pace than legacy physical credentials. These new credentials are mobile and biometric. COVID-19 accelerated demand for mobile-based and contact-free biometric applications. They are popular for their convenience, level of control, and advanced capabilities. In mobile systems, smartphone apps act the same as physical key cards and fobs. The app gets specific permissions for that device and user. Biometrics use varies by technology. For example, facial recognition requires users to position their faces for camera capture. Whereas retinal scanning usually requires looking through an eyepiece with low-energy infrared light.

Mobile credentials also have the benefit of connecting to device biometrics such as FaceID or TouchID to authenticate the user. This means that there is less opportunity for an unauthorized person with someone else's mobile phone to gain access. Biometric credentials rely on fingerprints, faces, iris scans, etc. to authenticate and validate the user. They are innate to the user and so much harder to spoof. With modern credentials, organizations have choice and convenience options that they can securely provide to their users.

PHYSICAL | PROS:

- Enterprises have widely adopted this technology
- There is an ample supply of affordable cards and fobs
- Easily provisioned for access points regardless of the number needed
- Can configure and reconfigure access using the same card

PHYSICAL | CONS:

- Credentials are not inherent to the user for authentication
- Sharing, losing, stealing, or duplicating the credential compromises security
- Added cost and managerial hassle issuing, collecting, and replacing physical credentials

MOBILE | PROS:

- Saves time and money not having to replace or collect card or fobs
- More sanitary due to lack of touching physical devices
- Convenience: most people carry a mobile or smartphone
- More secure: users are less likely to lend their phone as an access credential
- Administrators can create, revoke, and change access on a remote basis
- Offers multi-factor authentication, location awareness, and mass notification

MOBILE | CONS:

- Privacy issues may arise with device access and personal information

BIOMETRIC | PROS:

- Credential is inherent to the user and not shareable
- Easy to use
- Prices have become affordable (especially fingerprint and face recognition)
- Difficult to spoof

BIOMETRIC | CONS:

- May be more expensive than physical credentials
- Privacy concerns involving the storage of personal data
- Accuracy issues (false positives and negatives)
- Some technologies may seem invasive (e.g., retinal scans)

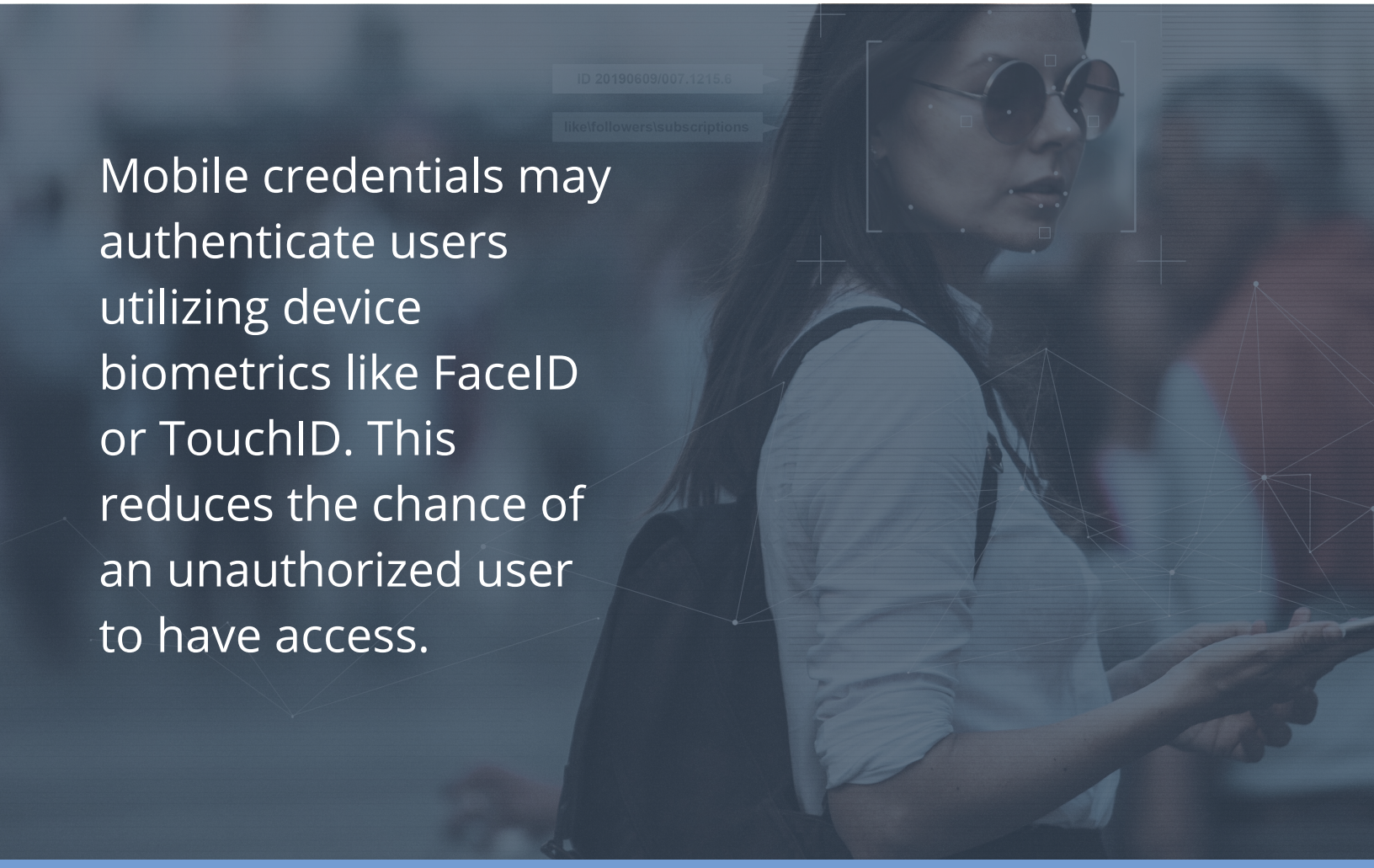
ADDITIONAL CONSIDERATIONS:

Frictionless – eliminates unnecessary high-touch surfaces, creates a frictionless user experience

Trust – credentials can be shared confidently and are not easily discoverable

Privacy – matches with organizational culture toward biometric data

Security – security levels to protect credentials from being shared, stolen, or hacked



Mobile credentials may authenticate users utilizing device biometrics like FaceID or TouchID. This reduces the chance of an unauthorized user to have access.

5 Stand Alone Video or Integrated Video Surveillance?

It is surprising that many enterprise organizations are still without adequate video surveillance as part of their facility management and security program.

How does an access control platform with video surveillance yield more efficient security? First, the addition of video surveillance enables businesses to track critical information. Second, video that is integrated with access control can provide a visual record of every access event. Third, these systems deliver transparency and accuracy in monitoring individuals as they move throughout a facility allowing security teams to monitor and act in the event of inappropriate access or behavior. What's more, integrated video surveillance allows facility and security management staff to work within a single interface without having to navigate between different systems.

Not all video surveillance systems are created equally. For organizations looking to modernize, cloud-based video surveillance provides an infinitely scalable solution for viewing live and recorded video and a variety of storage options to meet compliance requirements. Additionally, the advanced capabilities in video from AI-based search, face or object recognition, and more can enhance the overall security posture while also simplifying security and facility management.

INTEGRATED VIDEO SURVEILLANCE | PROS:

- Strengthens security platform value
- Simplifies facility and security management
- Enables advanced video features such as facial or license plate recognition
- Connects a visual to every access event for real time validation
- Supports quicker investigations

INTEGRATED VIDEO SURVEILLANCE | CONS:

- May be limited by which video managements systems are integrated with the access solution

ADDITIONAL CONSIDERATIONS:

Efficiency – Reduce time and effort to manage facilities by viewing in a single system

Safety – Respond to incidents and risks in real-time

Accuracy – Physical access control alone cannot provide accountability that video does

Centralization – Streamlined data collection to see everything at once

6 Stand Alone or Integrated Access Credentials?

When designing enterprise security, how to credential users is a weighty choice. Enterprise organizations must ensure that employees, contractors, and customers have the correct access to digital resources and data to manage and grow their businesses. This is partly to ensure the business can operate smoothly, but also to protect the digital assets from the largest single cyber-attack vector—stolen or compromised credentials.

However, most enterprises still manage the identities for physical access to facilities and spaces in a siloed manner not connected to the digital identity and access management solutions.
These identity and access management (IAM) systems can be paired with the physical security platform. Doing so balances accessibility and security in a powerful way.

First, it ensures that user access rights are up to date. As soon as an employee is onboarded, they receive the appropriate physical access credentials and entitlements. When an employee leaves a company, the system automatically revokes those entitlements and disables credentials preventing unauthorized access to physical spaces.

Second, integrating physical access with digital IAM solutions synchronizes access privileges to individuals and devices so that there is always an auditable view of all access throughout the organization for compliance reporting and real-time investigations.

Third, integrating digital and physical identities allows security personnel to focus on essential responsibilities and not spend time doing double entry for onboarding and offboarding users. Integrating physical security and identity management improves overall cyber and physical security.

STAND-ALONE CREDENTIALS | PROS:

- Lower platform expense

STAND-ALONE CREDENTIALS | CONS:

- Less current than integrated credentials and therefore less secure
- More time-consuming for security personnel to validate credential status with cross-functional teams

INTEGRATED CREDENTIALS | PROS:

- Highly accurate credentials
- Automated processes
- No manual intervention

INTEGRATED CREDENTIALS | CONS:

- Higher expense
- Upfront configuration
- Training and change management required

ADDITIONAL CONSIDERATIONS:

Greater control – Mitigate internal/external data risks with user oversight and visibility

Proficiency – Reduce the effort required to manually manage access control

Security – Ease of enforcing policies for user authentication, validation, and privileges

Compliance – Demonstrate on-demand auditing for regulatory compliance

7 Legacy or Modern Digital Visitor Management System?

Visitors, contractors, suppliers, and business associates need access to enterprise facilities. At the same time, the safety and security of employees is paramount. However, many enterprises are still using legacy—even paper-based—visitor sign-in processes which don't provide an audit trail of visitors in the facility. These old-school ways of managing visitors can create gaps in security protocols, especially during an emergency

When an enterprise deploys a modern visitor management system connected with its security platform, guests, and security staff both gain a better experience. A modern visitor management system makes visits convenient, efficient, and productive. It also limits access to specific spaces and controls visitor routes automatically.

Visitors can pre-register by sharing needed documents in advance. Once they arrive on site, they can log in themselves and receive a credential. The enterprise can maintain security for the duration of their visit because visitor routes and space access are intentional. Credentials can expire at a set time in an automated way. This guarantees that when visitors leave the property, they lose future access.

LEGACY VISITOR MANAGEMENT| PROS:

- Generates a log of visitors, even if using a paper-based system
- Easy to deploy
- Labor resources are the only direct cost

LEGACY VISITOR MANAGEMENT| CONS:

- Not auditable over long-term
- Time consuming and manual
- Not connected to access control system
- Doesn't track movement in case of an incident
- Likely requires an escort
- Requires a human to manage front desk and visitor entry points

MODERN VISITOR MANAGEMENT| PROS:

- Creates a welcoming, professional visitor experience
- Saves valuable staff time signing guests in and out of buildings
- Ensures that visitor logs are available to security personnel
- Connects with access control for automated credential provisioning
- Utilized modern credential technologies such as mobile passes or QR-based credentials
- Automated for an entry point without staff
- Connects with integrated workplace management and space booking applications

MODERN VISITOR MANAGEMENT| CONS:

- Requires additional expense
- Requires additional training
- May require cameras or other devices to fully automate

ADDITIONAL CONSIDERATIONS:

First impression – companies never get a second chance to make a first impression

Safety-centered – in the event of a crime or incident, visitor logs are more dependable and accessible

Deterrents – visitor management bolstered by video surveillance is a powerful signal to potential troublemakers

Experience matters – modern visitor management is connected to integrated workplace applications such as space booking, access credentials, room reservations etc

8 Legacy or Modern Access Control Systems?

During security planning, businesses must decide whether to maintain legacy systems or to upgrade them to modern ones. Legacy systems endure because they continue to function at an acceptable level. Administrators and users are comfortable using them. The enterprise understands their costs and benefits. Keeping legacy systems also postpones the expense of migration, replacement, or integration.

As time goes by, both hardware and software grow harder to maintain, upgrade, and replace. For example, they may depend on proprietary or obsolete operating systems or hardware. Some organizations work to replace elements of legacy infrastructure over time. Sometimes, this saves money. In other cases, this approach salvages an odd array of hard-to-manage hardware and software.

Modern applications and systems provide flexibility. They can merge siloed systems to create an integrated software platform. This is crucial because it removes the juggling of disparate databases and portals. There are major benefits when network elements work together. This eliminates the need to rip-and-replace. With modern systems, businesses can match service delivery with demand – to meet business needs.

LEGACY | PROS:

- May be necessary for mission-critical systems or to fulfill specific business operations
- Contain valuable historical data and file setups
- Staff and administrators are comfortable with their use

LEGACY | CONS:

- Often obsolete and outdated in compliance with standards
- Can be expensive to maintain
- Lack of support, patches or updates creates vulnerabilities
- Scarcity of developers familiar with technology and programming
- Likelihood of incompatibility with new systems and components
- May be exclusive to a vendor and its partners
- Customization can be complex, expensive, and limited

MODERN | PROS:

- Easy to implement with consistent business processes and lower technical barriers
- Ensures data is always available, improving productivity and efficiency
- Provides scalability so you can add or subtract resources
- Easy access and restore from back-up
- Provide business value in the form of useful data

MODERN | CONS:

- A new provider may not offer all the desired features or customizations
- It requires reliable connectivity and an internet connection
- Outages can disrupt accessibility and operations
- Proprietary systems or vendor networks may limit your options

ADDITIONAL CONSIDERATIONS:

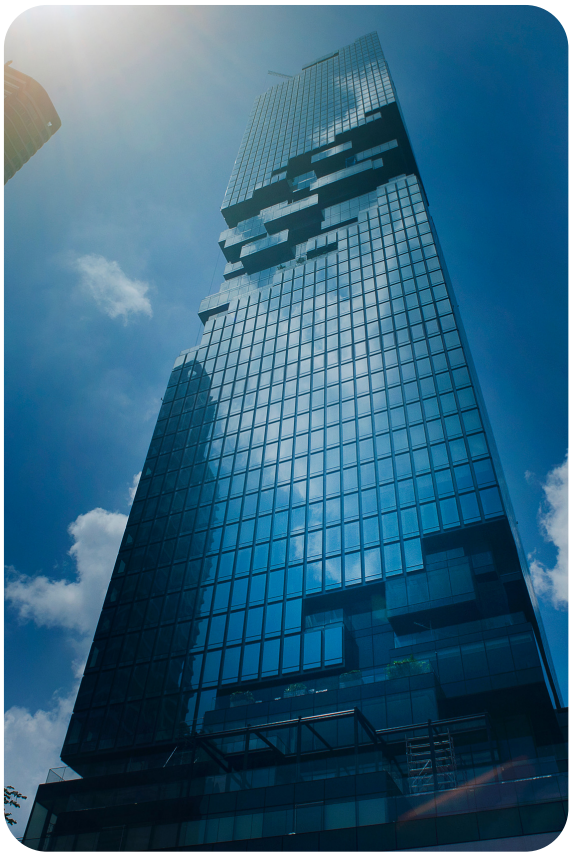
Scalability - applications need to scale to user demand, across multiple locations

Flexibility - applications need to function across multiple environments

Resilience - ensure data and user experience are protected in the event of disruptions

Availability - ensure maximum uptime with several points of failure

IS **ACCESS CONTROL** MODERNIZATION RIGHT FOR YOUR ENTERPRISE

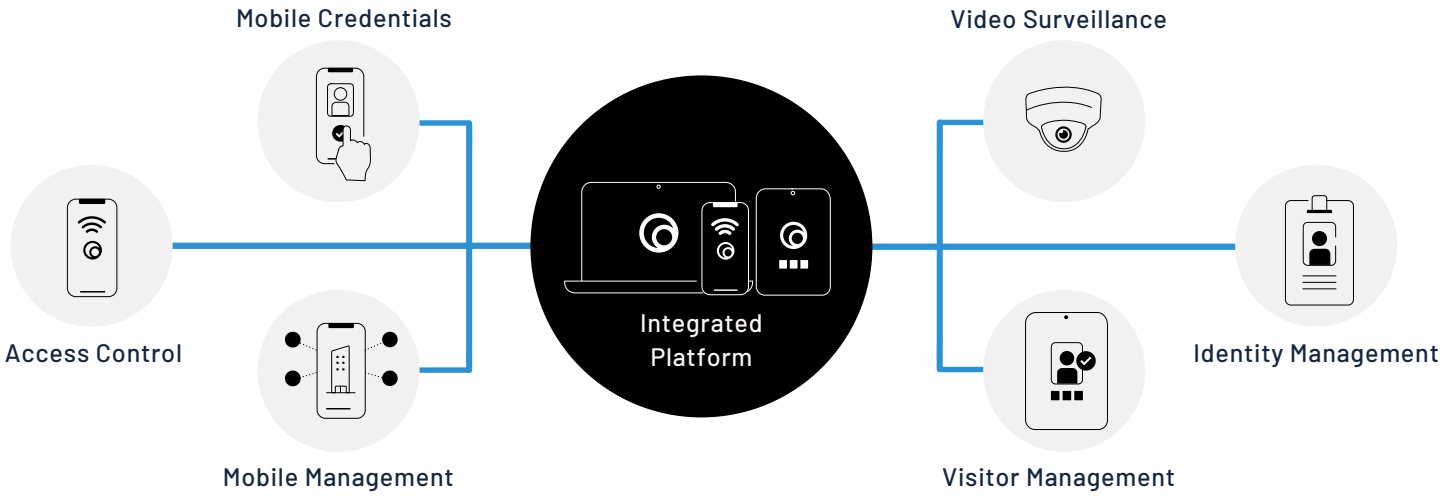


A modern access control platform is a superior choice for your enterprise if you need:

- Consistent access control over multiple facilities or geographies
- Remote administrative access from anywhere at any time
- Automated system maintenance, updates, and upgrades
- Modern and more secure credentialing and identity management
- Flexibility to restrict or adjust user access for efficiency and emergency management
- Integration into adjacent systems such as visitor management, workplace apps like desk booking and resource scheduling, IAM and more.

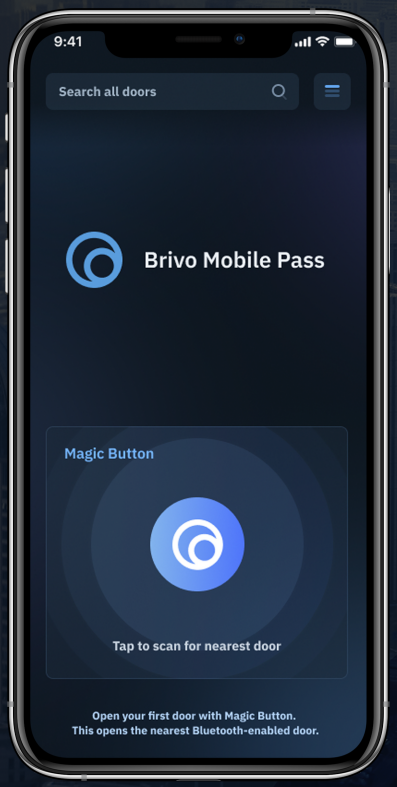
See How Brivo Can Help

If an access control modernization is right for your enterprise, we urge you to evaluate Brivo. Brivo has been the leader in cloud-based access control for the past 20 years. Brivo is secure, partner-centric, and committed to service excellence.



BRIVO BY THE NUMBERS

- **300M** square feet of real estate protected in **40+** countries
- Supporting **70K+** deployments worldwide
- An open and extensive **integrated tech partner ecosystem**
- **1M+** Mobile Credentials
- **10+ years** of cyber security audits
- **800** Developer using our API
- **1500+** Authorized Dealers



WHY BRIVO

Brivo, Inc., is the global leader in mobile, cloud-based access management and smart spaces platforms serving commercial real estate, multifamily residential and large distributed enterprises. Brivo's building access platform is the digital foundation for the largest collection of customer facilities in the world, occupying over 300 million square feet across 42 countries. Learn more at www.Brivo.com

visit brivo.com

Request a Consultation

schedule it

brivo

contact us to get started:
sales@brivo.com