ALLEGION™

Exploring the benefits of wireless

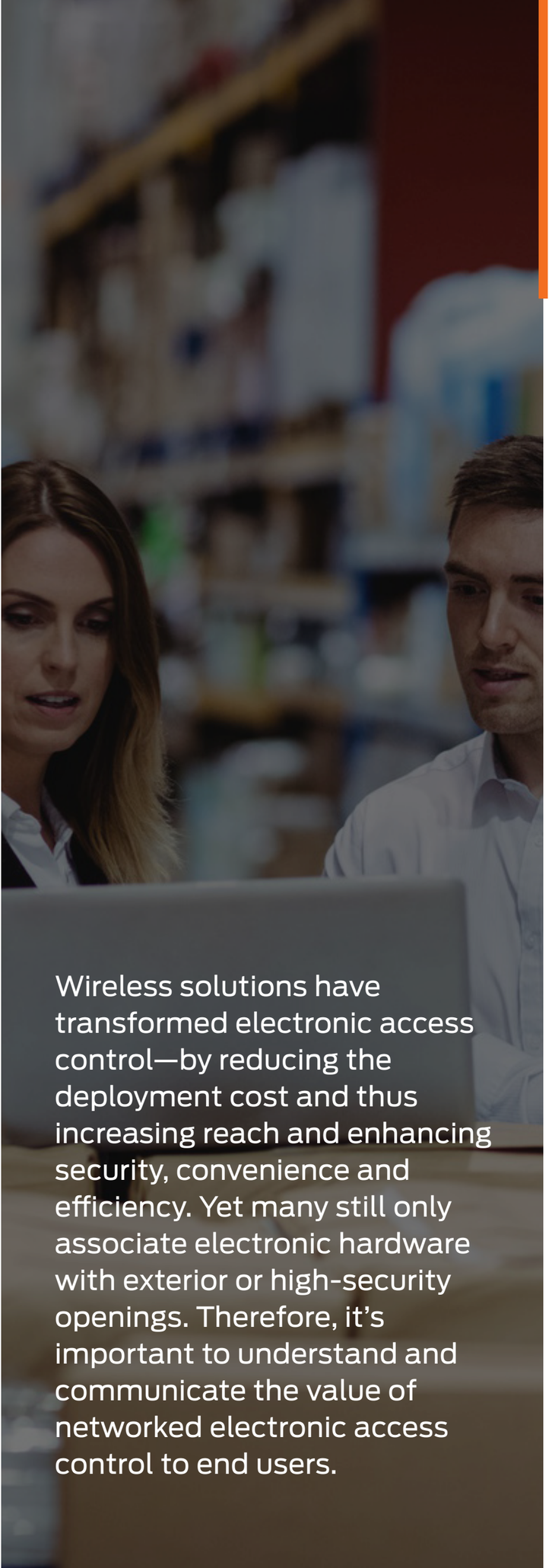
For commercial security integrators and your customers

Introduction and Table of Contents

Customer needs are expanding. Fortunately, technology is also evolving to aid your ability to exceed their expectations. Customers are looking for solutions that offer value beyond security, including operational efficiency and convenience for their internal users.

Wireless technology enables you to serve your customers in ways that were previously not feasible. Electronic access control is no longer intended only for high-security, exterior openings. Wireless devices extend the benefits of electronic access control to interior doors to improve the user experience—while providing additional revenue opportunity per project.

These materials explore the benefits of adopting wireless as part of your business offering and provide additional resources to help communicate this additional value to customers, including application examples



Wireless solutions have transformed electronic access control—by reducing the deployment cost and thus increasing reach and enhancing security, convenience and efficiency. Yet many still only associate electronic hardware with exterior or high-security openings. Therefore, it's important to understand and communicate the value of networked electronic access control to end users.

Benefits of wireless to end users

Control

Users can configure locks, manage access rights and assign schedules from virtually anywhere, which means more command of their facilities as a whole.

Visibility

Users have access to audit trails and alerts; utilizing real-time data and technology allows them to manage their facility as well as the staff or occupants within it.

Deeper connectivity

Even if your customers aren't looking for a complete smart building solution today, paint the picture of what's possible when networked wireless locks are integrated with other sensors and smart devices.

Easy adoption

Wireless locks complement existing security solutions and can be tailored to fit varying security needs; including different architectures depending on the application.

Key management

Switching to electronic credentials improves efficiency and security. Mechanical key override can still be an option, but facilities can reduce the distribution of those keys to a few individuals.

Convenience

When electronic access control is implemented throughout a facility, a single credential can provide a frictionless experience while users move from one space to the next with ease.

Future growth

The way in which access control is monitored and the solutions available evolve year after year. An open architecture allows end users' security solutions to evolve along with advancing technology and the changing needs of their facilities.

Flexible options to fit customers' needs

Real time and Wi-Fi based offline solutions

Real-time network benefits

- Highest levels of security control providing bi-directional updates for event notification and access changes along with real-time lockdown capability
- Flexible solutions include two options for real time communication
- Number of users and audits is dependent on access control solution and can be unlimited

Wi-Fi offline network benefits

- Convenient and efficient remote management with daily scheduled updates
- Updates occur automatically once or more daily between host and door, for capture of historical events and remote access changes
- The locking device manages access based on latest update from access control software
- Bluetooth mobile device compatibility allows option for immediate updates to be made at the door

Now real-time network solutions allow 2.4 GHz and 900 MHz wireless devices to co-exist

900 MHz solutions

- Longer wavelength 900MHz enabled devices connect wirelessly to the Panel Interface Module (PIM)
- Superior penetration in typical building construction
- Wireless range up to 200 feet to devices with up to 1000 feet possible in line of sight
- High gain antenna options can achieve line of sight distances up to 4000 feet
- RS-485 connection through Access Control Panel (ACP) to host
- Access control software manages all device commands and enables lockdown capability

Bluetooth 2.4 GHz communication

- Bluetooth enabled devices can connect wirelessly to the ENGAGE™ Gateway
- Range up to 30 feet from gateway to device
- Multiple ways to connect gateway to host:
  - Ethernet connection direct to host with redundancy present in device
  - RS-485 connection through Access Control Panel (ACP) to host
- Access control software manages all device commands and enables lockdown capability

The impact of incorporating wireless solutions into your business

Wireless access control products may initially be perceived as limiting revenues when narrowly comparing the price per door. In practice, including these solutions in your portfolio can significantly improve both revenue and profitability. By incorporating wireless solutions, projects can be completed quickly and with a smaller labor force, which means billing and payments occur in a more timely manner. This potential increased cash flow and profit margin can allow integrators to grow their business more effectively.

Let's explore.

1. **Recurring monthly revenue (RMR).** Steady, recurring revenue indicates more predictable profitability in the future. Wireless solutions set up the foundation for RMR. Continue reading.

2. **Security convergence.** Wireless solutions enable the access control system to expand to applications that likely would remain mechanical and unmonitored. This improves the customer's environment and the value of your relationship. Continue reading.

Expanding recurring monthly revenue

Security Sales and Integration's Recurring Revenue Report found that 18 percent of the 100 security companies surveyed reported that 41-50 percent of their total revenue was comprised of RMR. It states that while the average is closer to 35 percent of total revenue, more than a quarter of the companies reported greater than half of their revenue is credited to RMR.

This is a shift from the traditional business model where the customer purchased $12,000-20,000 of hardware from the integrator and then paid for the labor of installation. When services like video came along, the industry realized that end users were less concerned about the specific product installed than the service provided. Instead of asking for a cash outlay and capital investment, dealers realized they could charge a smaller monthly fee.

Operational expenses, which allow customers to pay as they go for the services, offer greater flexibility to accommodate for changing security needs with fewer budget complications. A capital expense where everything must be paid upfront typically requires allocating funds and longer approval processes.

This model allows integrators to charge recurring fees for access control services at lower price points. The integrator enjoys a reliable revenue stream, and customers are happy about not having a large upfront expense. In addition, this model opens the door for dialogue with customers about outsourcing more activities as a managed service agreement to their integrator. This could include credential management, physical security monitoring and other responsibilities that may have previously been allocated to customer personnel. Beyond access control, security integrators are able to offer a number of monitored services, from cybersecurity to fire alarms to IT communications.

Predictable, repeatable revenue

As the security industry continues to increasingly engage with IT-centric decision makers, we will see customers shift focus from product to service-based minded solutions. As a result, the business model of monthly recurring or even managed access control will increase and have a big impact on overall margins.

Solutions like networked wireless access control further increase this opportunity for integrators. While the integrator's margin dollars per door may be lower compared to a traditional electrified solution, wireless locks allow end users to connect more openings within the same cost parameters. That sets up the foundation for RMR. Integrators are able to obtain a fee per connected device they are supporting. Without wireless, the customer's budget might have only allowed for there to be two or three points of service, totaling less than $30 per month. With wireless devices, end users can obtain the benefits of electronic access control on multiple additional application openings while increasing the recurring revenue opportunities for integrators by roughly three times or more per month.

Reduced barrier to adoption

Large upfront costs can be intimidating to customers. Manageable monthly payments are an attractive alternative that breaks down adoption barriers for some customers, enabling them to afford the desired services. Again, capital expenses often require more planning and approval versus operational expenses that occur throughout the year.

Beyond a reliable and predictable revenue stream, recurring monthly revenue offers a number of benefits for improving business. Start by looking at opportunities to grow with the existing contacts. It can't be a one-time sales approach. Considers customers in light to medium commercial facilities that couldn't justify access control before. Would a monthly plan open up incremental opportunities with these users? There are some barriers to overcome at first, but security integrators that utilize the RMR model—emphasizing service as their value proposition and establishing broader relationships—are likely to see business growth in the long run.

Security convergence

Innovative advancements have created exciting capabilities, the most successful of which offer conveniences that make daily routines simpler and more productive. Keeping up with the latest technologies can sometimes lead to a mechanical vs. electronic mindset—out with the old and in with new.

With access control, it's more advantageous to consider how the two can complement each other—for the end user and integrator. The new doesn't always need to replace the old; not all mechanical needs to be upgraded to electronic. That said, it's likely the end user could benefit from the added value of electronic access control on select openings. Integrators with an understanding of electronics, especially wireless, are positioned to help their end users upgrade traditionally mechanical doors to include electronic access control for an enhanced user experience.

The evolution

As technology evolves, new features are introduced that complement a product's fundamental purpose. For example, think about the automobile. Its intended purpose is to get you from point A to point B. Today, we have GPS and built-in screens to make travelling to the destination simpler and more enjoyable. The same is true for a lock. Today's electronic access control solutions offer an added level of keyless convenience for occupants. The security and reliability of the mechanical solution are the foundation, but now facilities have data about who entered a space. They also have the enhanced security of electronic key control by limiting the distribution of mechanical keys. And with the rise of wireless electronics, these benefits are achievable on more doors than ever before. End users can afford to implement wireless electronic access control throughout a property, including interior doors. This allows integrators to service a greater number of doors compared to hardwired locks.

Striking a balance

Ultimately, the decision to introduce electronics should be based on the needs for each opening. The goal is to create a cohesive user experience that strikes the right balance of security, convenience and efficiency at every opening. To achieve this, it is important to understand when to select mechanical, wireless electronic or wired electrified.

It's easy to think that the same solution can be applied to all openings, but it's important to tailor the experience to each point in the facility to maximize the experience. The end user might have hardwired electronic locks on the main doors and mechanical everywhere else. The integrator's job is to educate them on the opportunities available and recommend where to upgrade for added convenience or control.

It's likely there are more opportunities to upgrade to electronics than first thought. Start by considering the purpose of the facility. Then figure out the needs of each door, starting at the perimeter and working your way inside. Think about the importance of security at the opening. What about ease of access? How often do access privileges change? How many keys are distributed for a given door? And, what is the frequency of use? For application examples, view page 8. Or read more about the wireless convergence.

Example market applications

Medical facilities

- IT room
- Supply rooms
- Labs

Commercial facilities

- Conference rooms
- Office entry
- IT room

Education facilities

- Classroom
- Auditorium
- Perimeter opening
- IT room
- Science labs/computer rooms

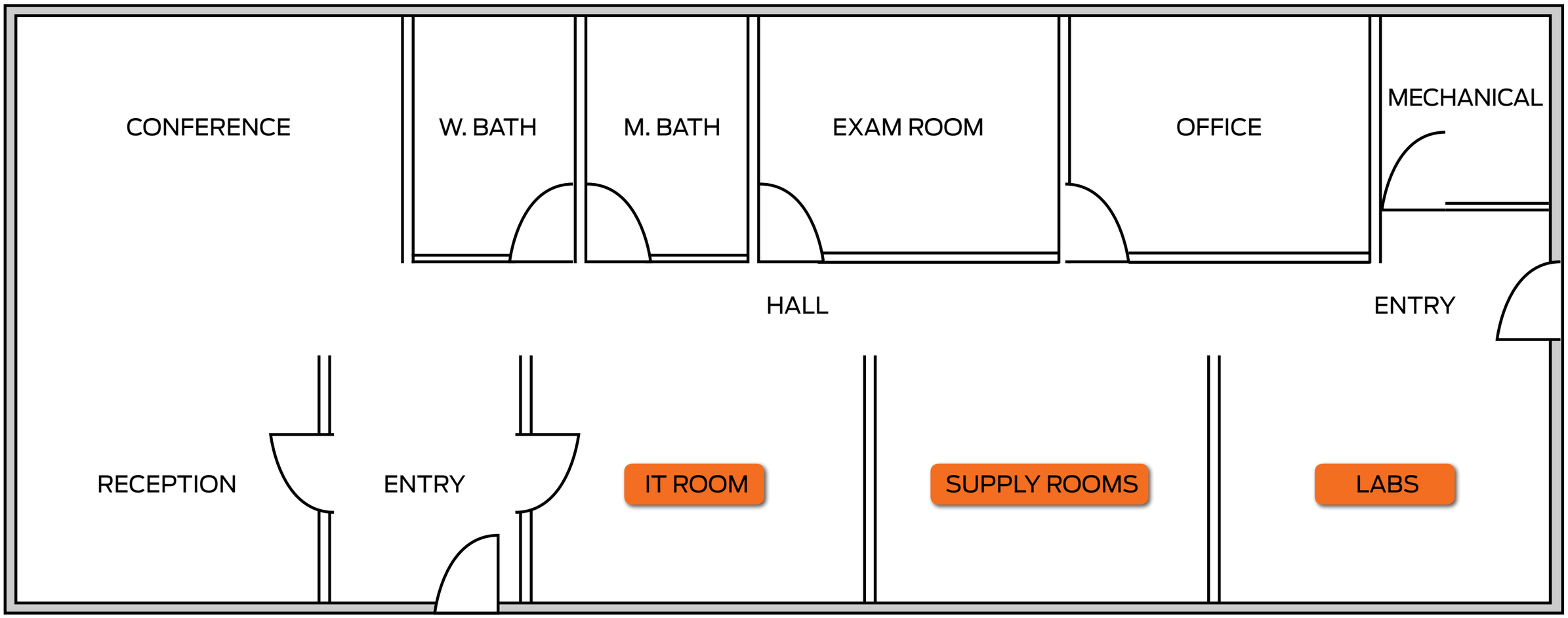
Assisted living facilities

- Resident rooms
- Restricted areas
- Secondary perimeter opening

Medical facilities

Outpatient, testing and other small hospital environments have several restricted areas that must be secured. Wireless electronic access control makes it easy for medical personnel leverage electronic credentials to to move between restricted and public areas easily. Real-time data and audit reports increase control and visibility throughout these facilities to secure the staff, occupants and assets inside. And with the amount of confidential information stored inside, it's important to mitigate risks associated with lost or stolen mechanical keys.

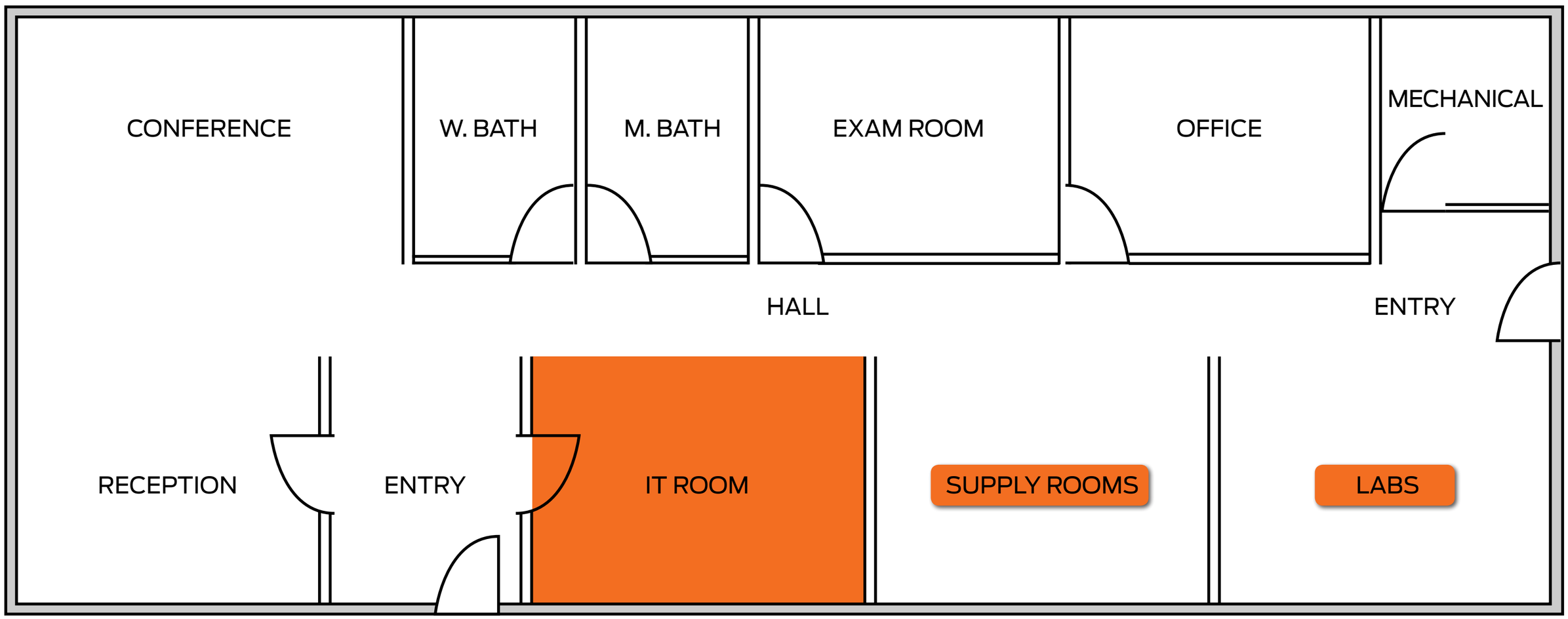
Applications to consider when speaking with end users include patient procedure rooms, testing labs, suite entry, cross corridor doors and storage spaces. Click on a room to learn more.



Medical facilities

IT rooms

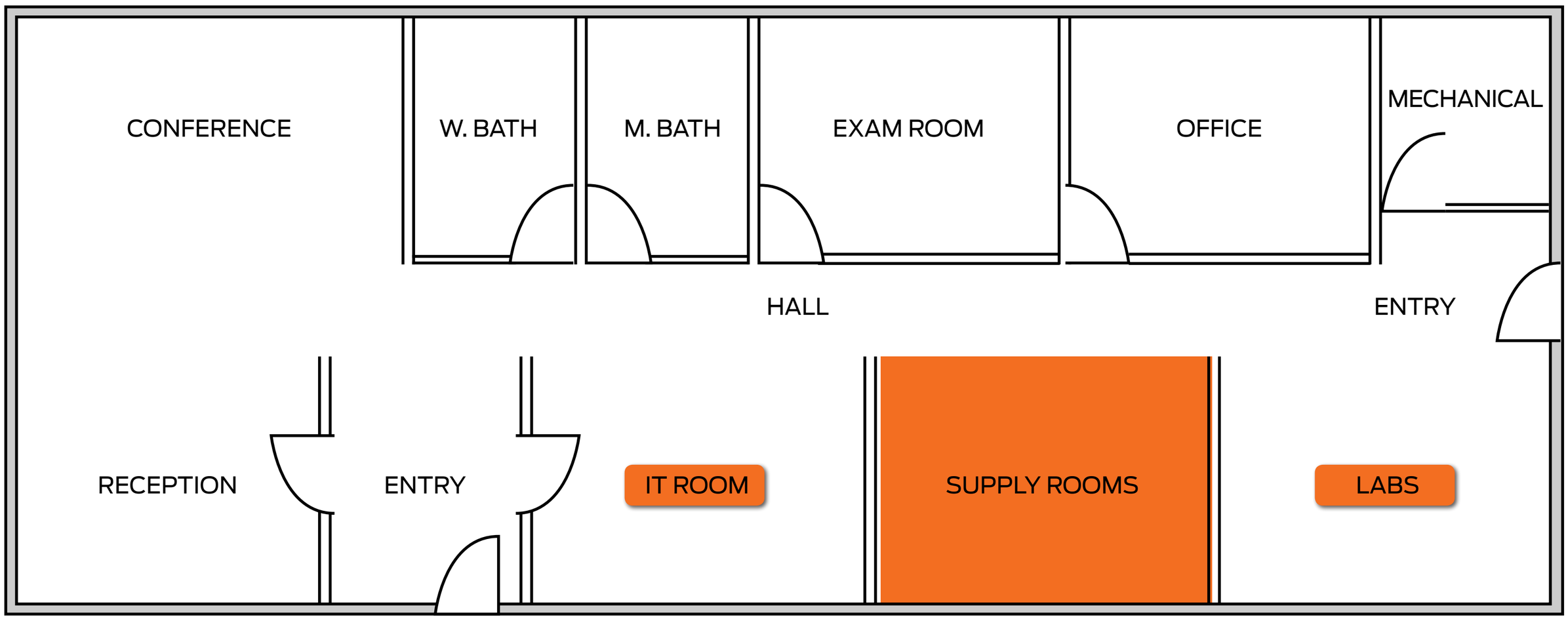
IT rooms, such as data closets or server rooms, contain sensitive information and expensive equipment. Wireless solutions make it convenient to control and monitor access to these spaces, which often need greater security than conference rooms and are only accessible by a small group. Real-time visibility provides reference of who request access to the room and when.



Medical facilities

Supply rooms

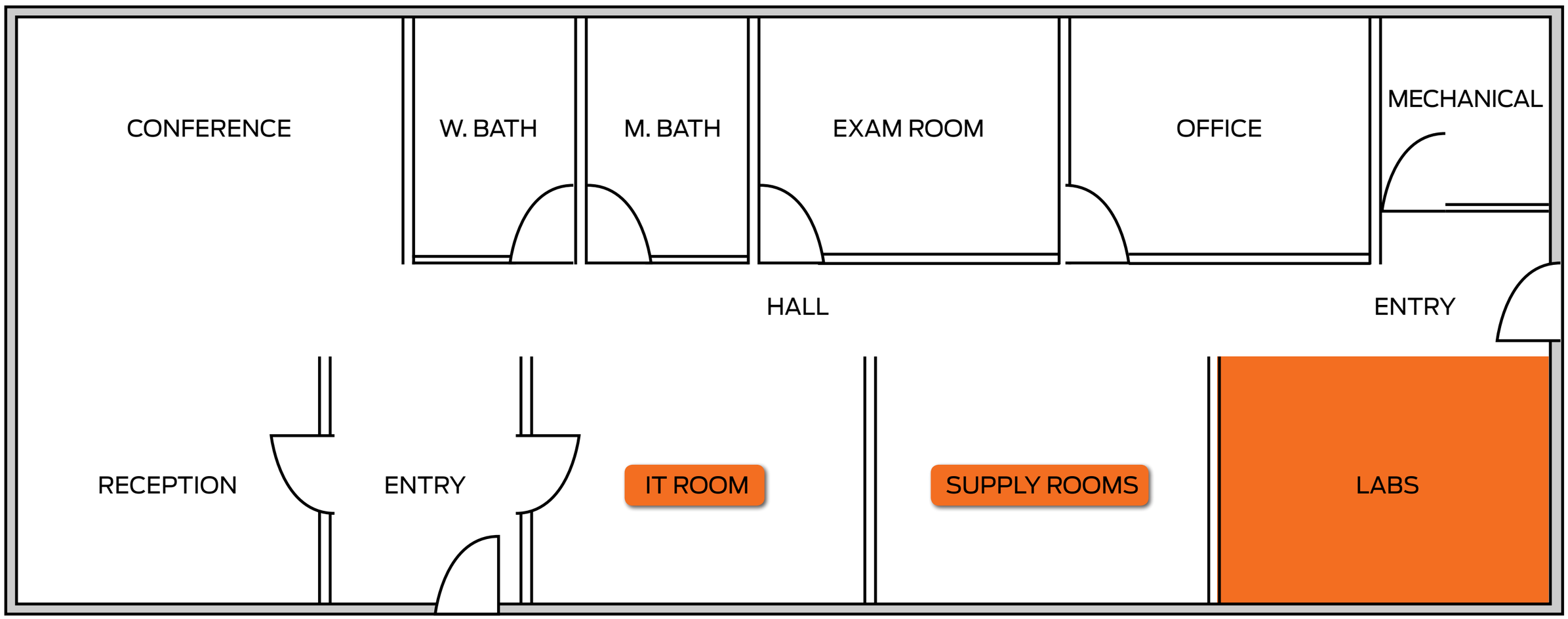
Staff-only spaces like supply rooms require enhanced security. Wireless solutions make it convenient to control and monitor access to these spaces. Staff is able to use the same credential that's used throughout the rest of the building. Audit reports can also be pulled to see who accessed the supply rooms as needed.



Medical facilities

Testing labs

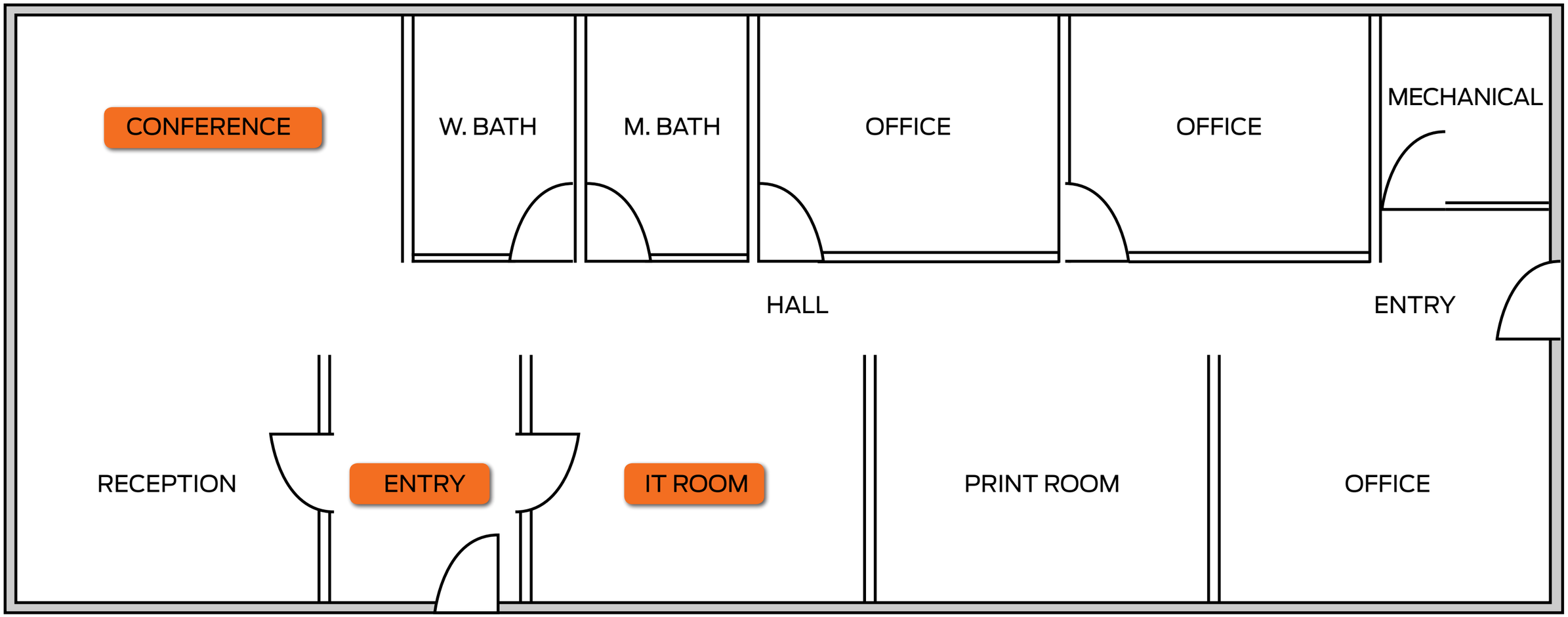
A select group of medical personnel is granted access to laboratories and pharmacies as they contain restricted assets like patient records, research and pharmaceuticals. Because these assets are off-limits to the majority, it's important to know who accesses a space and when. Electronic access control mitigates risks associated with lost or stolen keys and provides detailed audit trails and real-time data that's not available with mechanical solutions.



Commercial facilities, small to medium

Many commercial facilities have electronic access control at the perimeter and main entrances, yet there are many benefits that also apply to interior applications. General admittance is needed for shared spaces, while other areas need customized entry access. Wireless electronic access makes it simple to manage credentials and grant access rights electronically in place of mechanical keys for everyday use. In addition, end users benefit from improved convenience of using a single credential throughout the building.

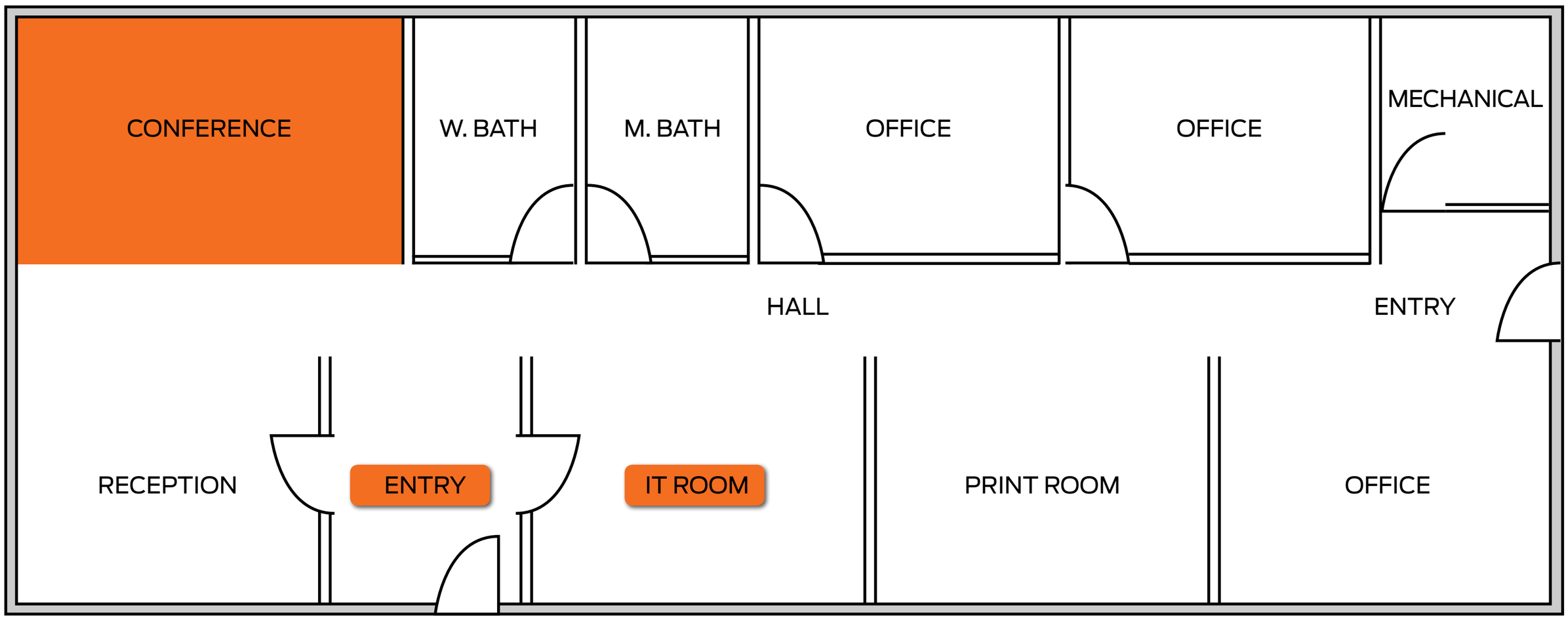
Applications to consider when speaking with customers include suite entries, offices, conferences rooms, IT rooms, storage closets and corridors. Click on a room to learn more.



Commercial facilities, small to medium

Conference rooms

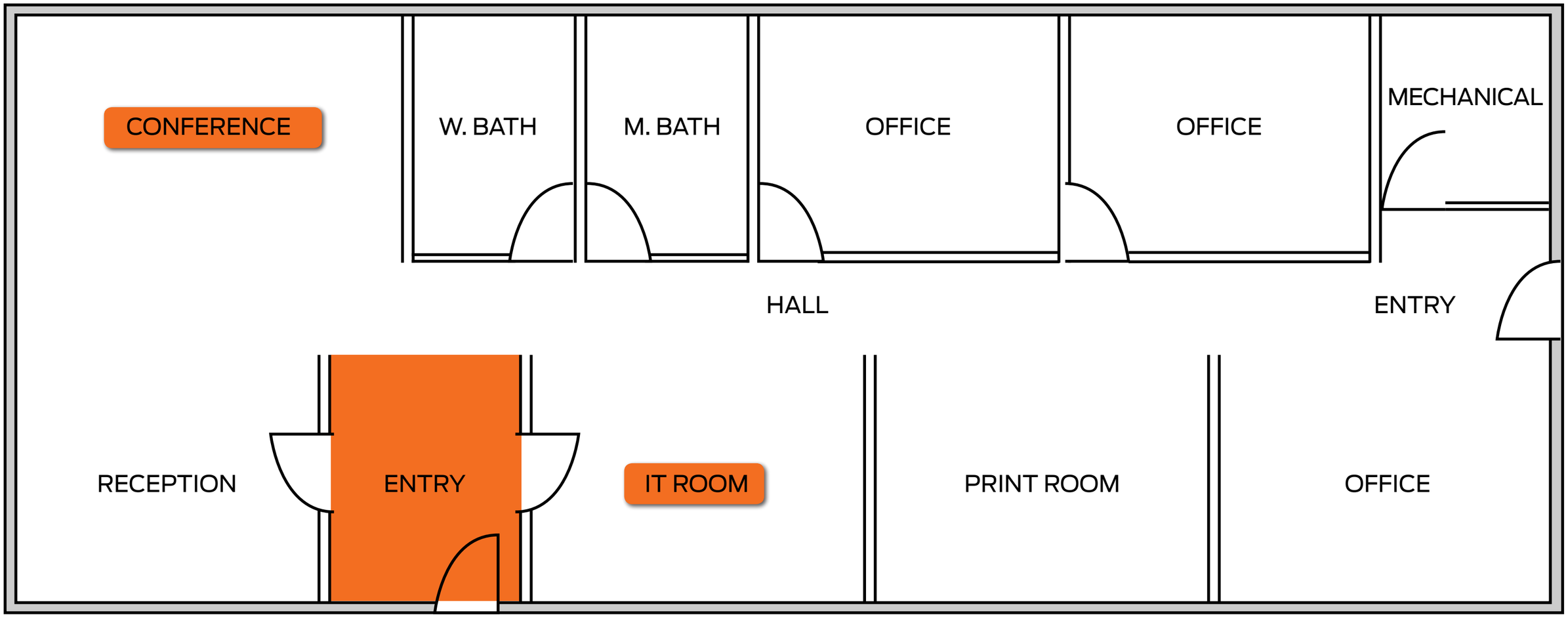
Shared spaces like conferences rooms are typically accessible to all employees. That said, there might be assets like AV equipment that need protected or the desire to limit times of access for specific groups to the room. Electronic access control provides additional security and improves convenience over mechanical keys to manage access to a select group of employees. Additionally, electronic access records can provide data about the utilization of shared spaces and even enable the customization of environments based on the users present.



Commercial facilities, small to medium

Office entry

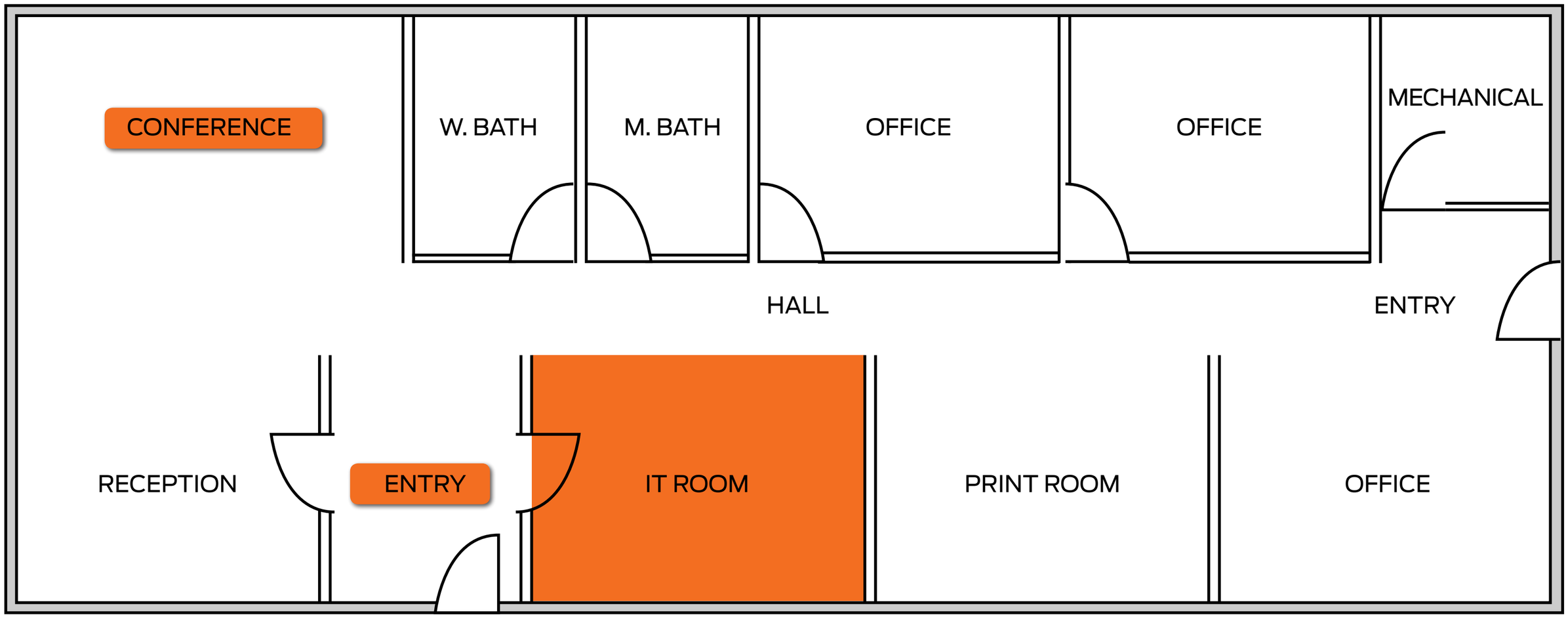
Unlike shared spaces, office entries are typically accessed by a smaller set of people. Electronic access control makes it easy to secure offices using the same credential that's used throughout the rest of the building for improved convenience.



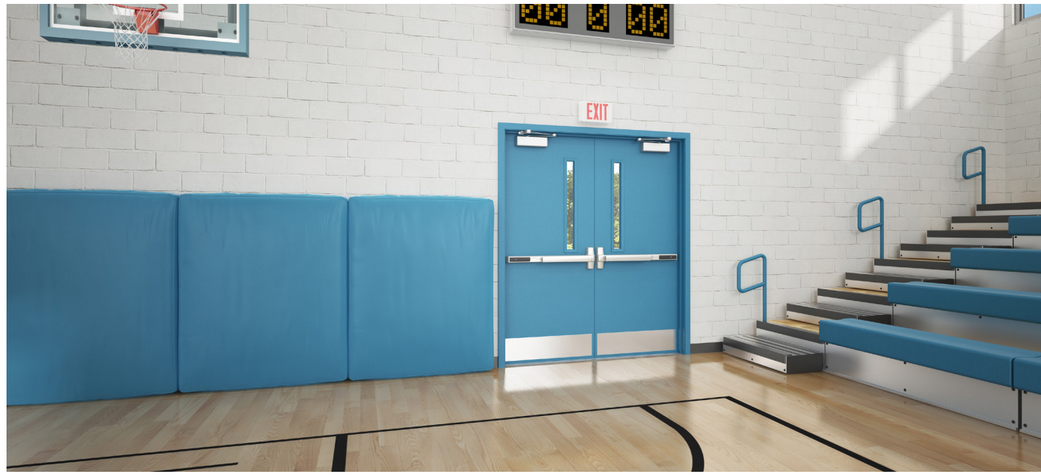
Commercial facilities, small to medium

IT rooms

IT rooms, such as data closets or server rooms, contain sensitive information and expensive equipment. Wireless solutions make it convenient to control and monitor access to these spaces, which often need greater security than conference rooms and are only accessible by a small group. Real-time visibility will provide reference of who request access to the room and when.

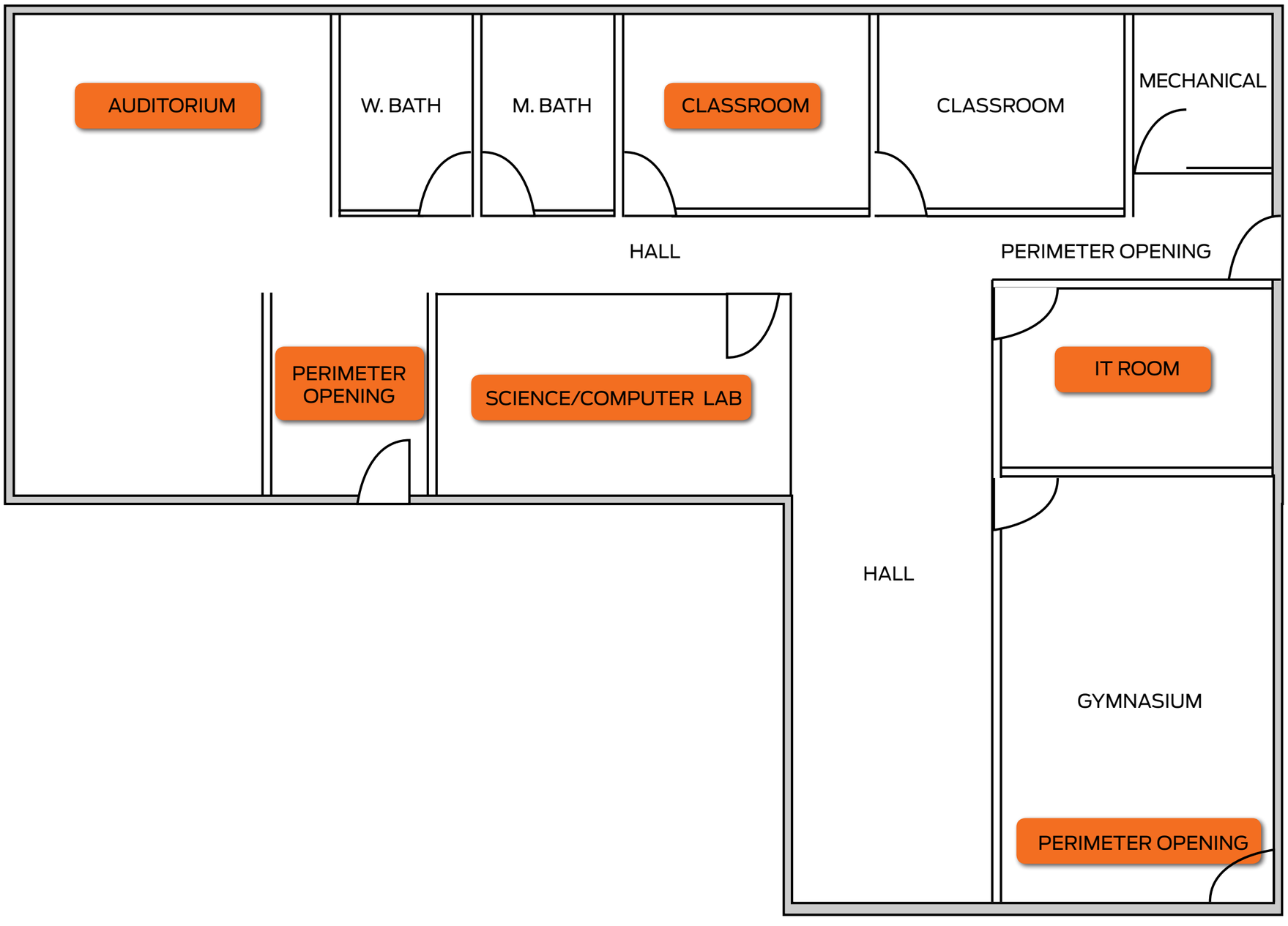


Education facilities



K-12 and higher education campuses face unique challenges to keep students, faculty and physical assets safe while mitigating operational costs. Wireless devices expand the reach of electronic access control to more openings—including validated, scheduled lock-up and emergency lockdown. They also make it simpler to manage locking schedules across campus and reduce the need for manual touring with mechanical keys. Allegion recommends taking a layered security approach. Talk through each layer with the end user and determine which tier of coverage makes sense for each.

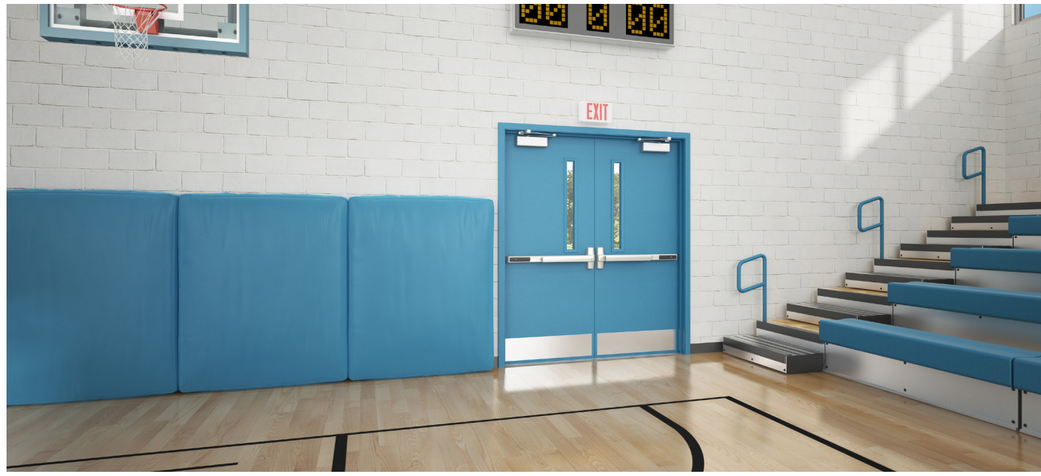
Applications to consider when speaking with end users include classrooms, auditoriums, residence halls, storage rooms, IT rooms, faculty spaces and meeting rooms. Click on a room to learn more.

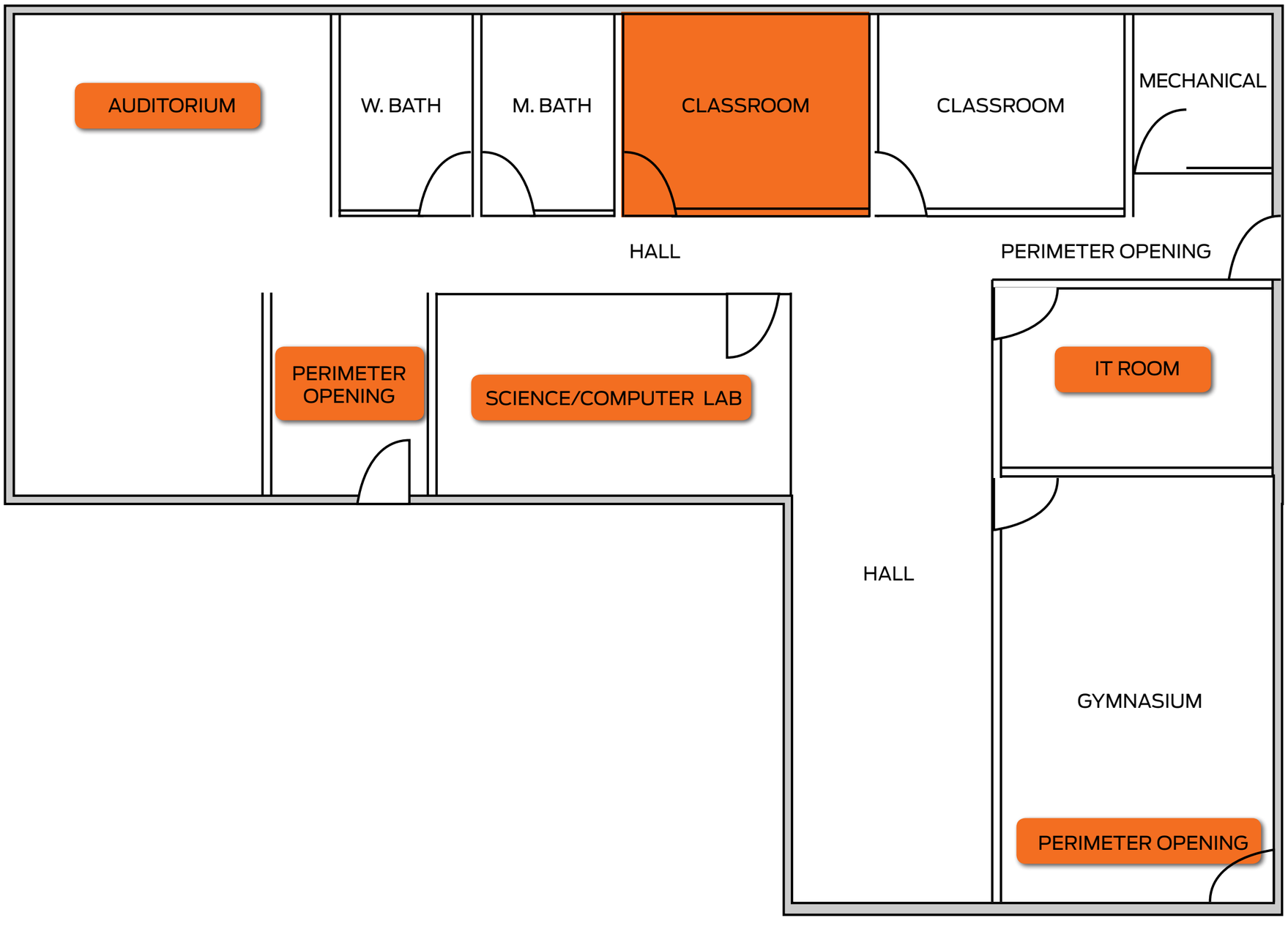


Education facilities

Classroom

When aligned with a school's protocol and budget, wireless electronic access control gives schools greater control over their classrooms. Electronic locking systems can be initiated both remotely or by a teacher in the classroom, ensuring quick responses during emergency situations.

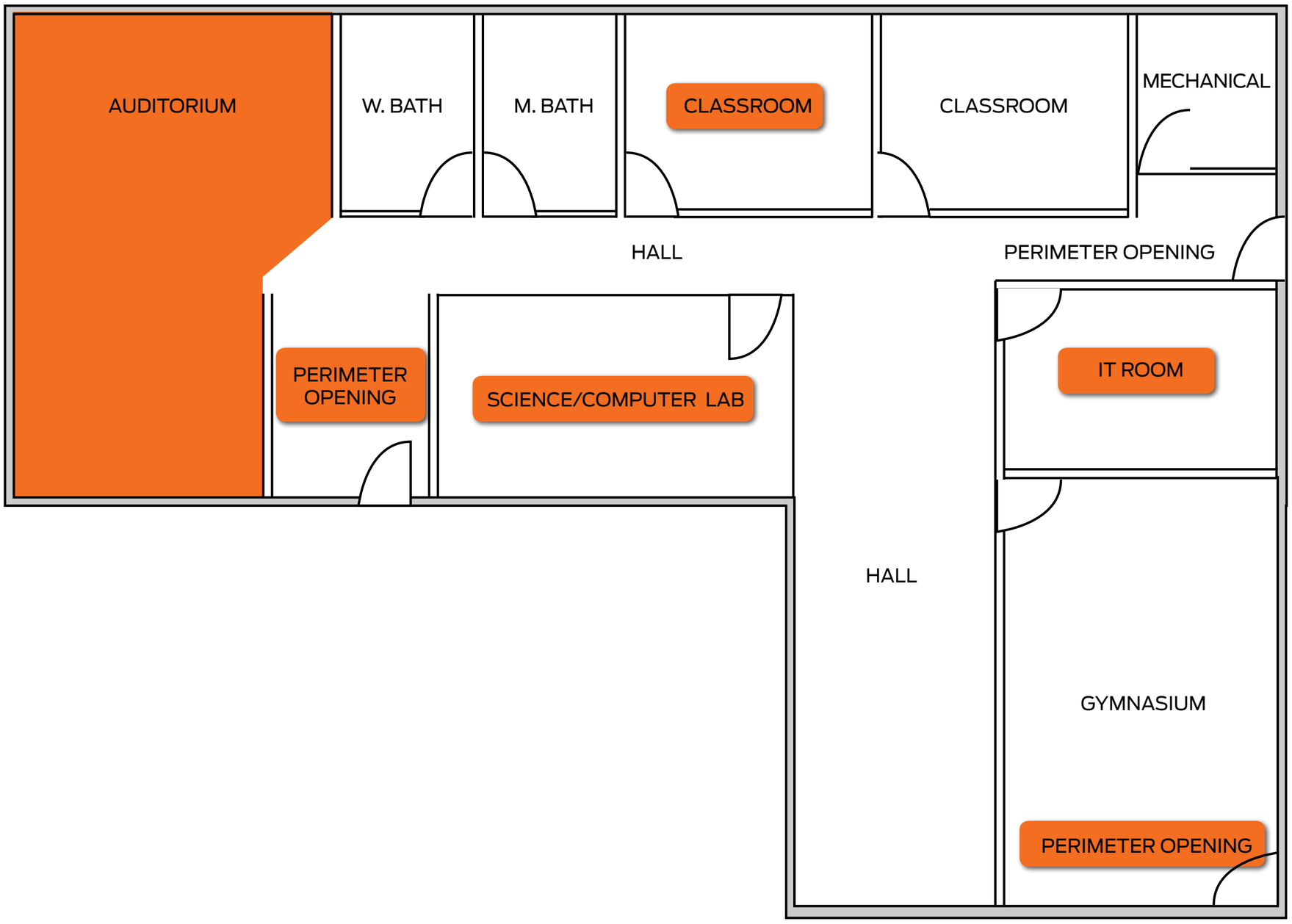




Education facilities

Auditorium

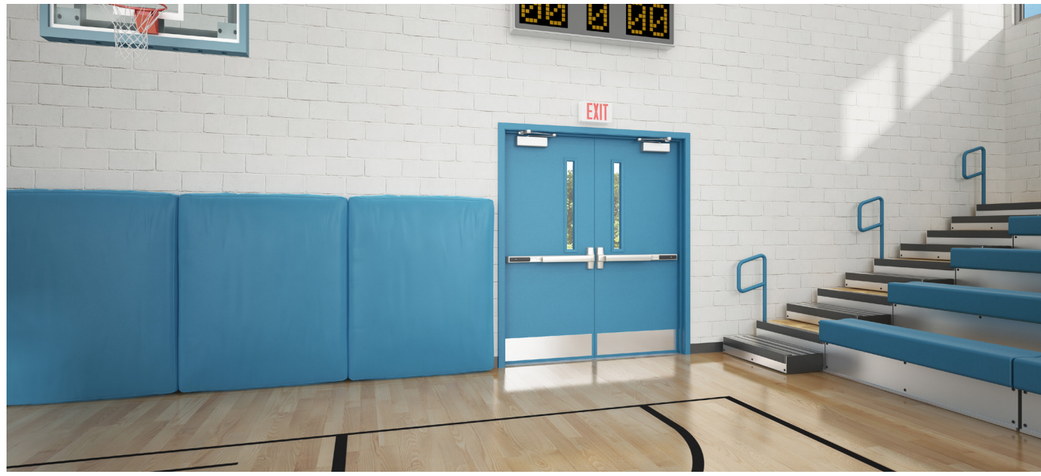
Auditoriums are accessible to students and staff during a majority of the day. Security needs change during performances and other large gatherings, some of which occur after normal hours. Consider electronic access control and monitoring on some or all of these openings. It reduces the time and costs associated with managing schedules and the distribution of mechanical keys.

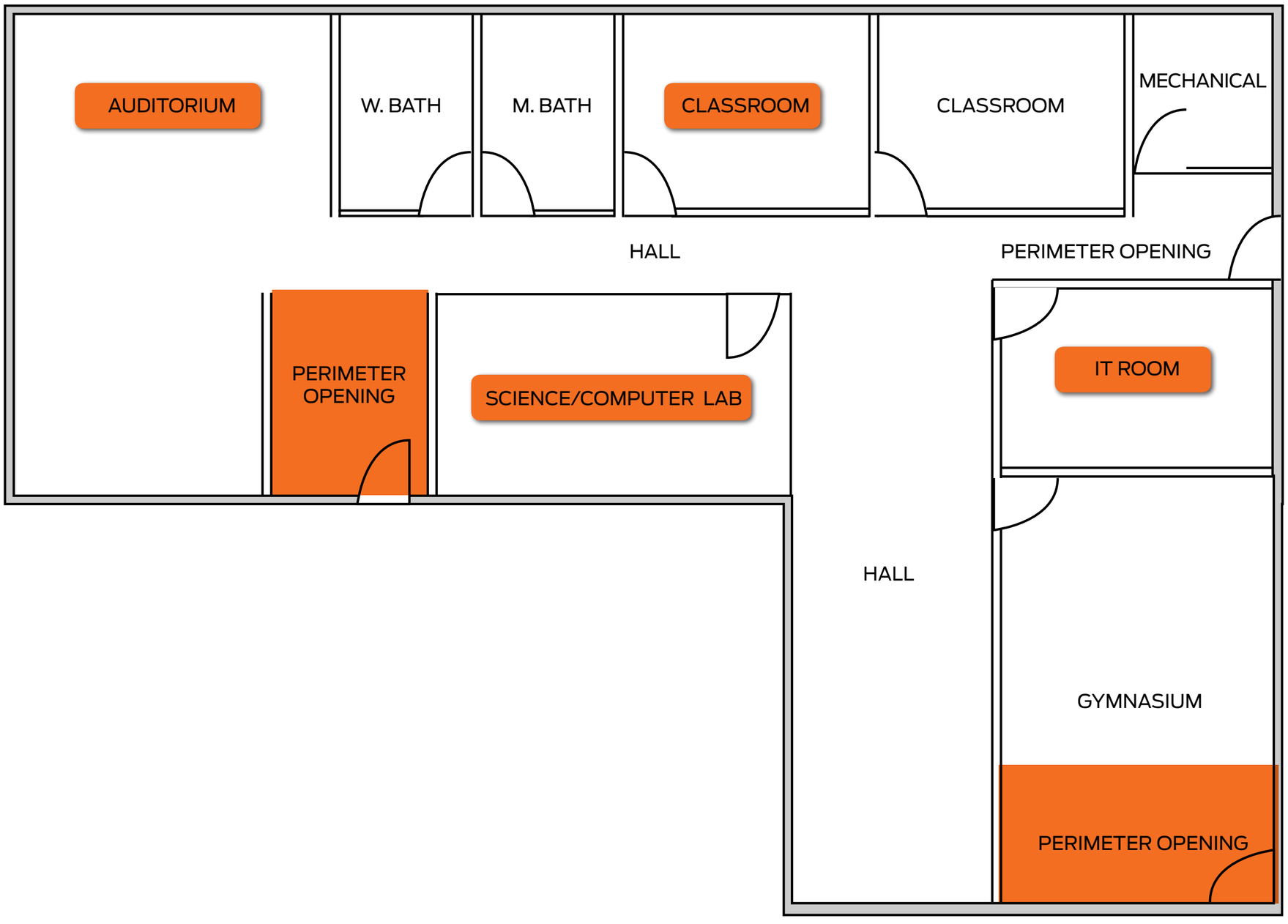


Education facilities

Perimeter openings

Education facilities typically direct traffic to designated controlled access points as best practices. While these primary openings are typically monitored and accessed electronically, there are additional secondary perimeter access points around the building that need to be considered. Historically, mechanical solutions are implemented on these openings due to the cost of electronic options. Wireless monitoring and access control solutions enable end users to enhance the security of these access points with retrofit solutions and remove the need to have to faculty physically visit the door to ensure it is secured. Learn more about the Von Duprin Remote Undogging and Remote Monitoring options.

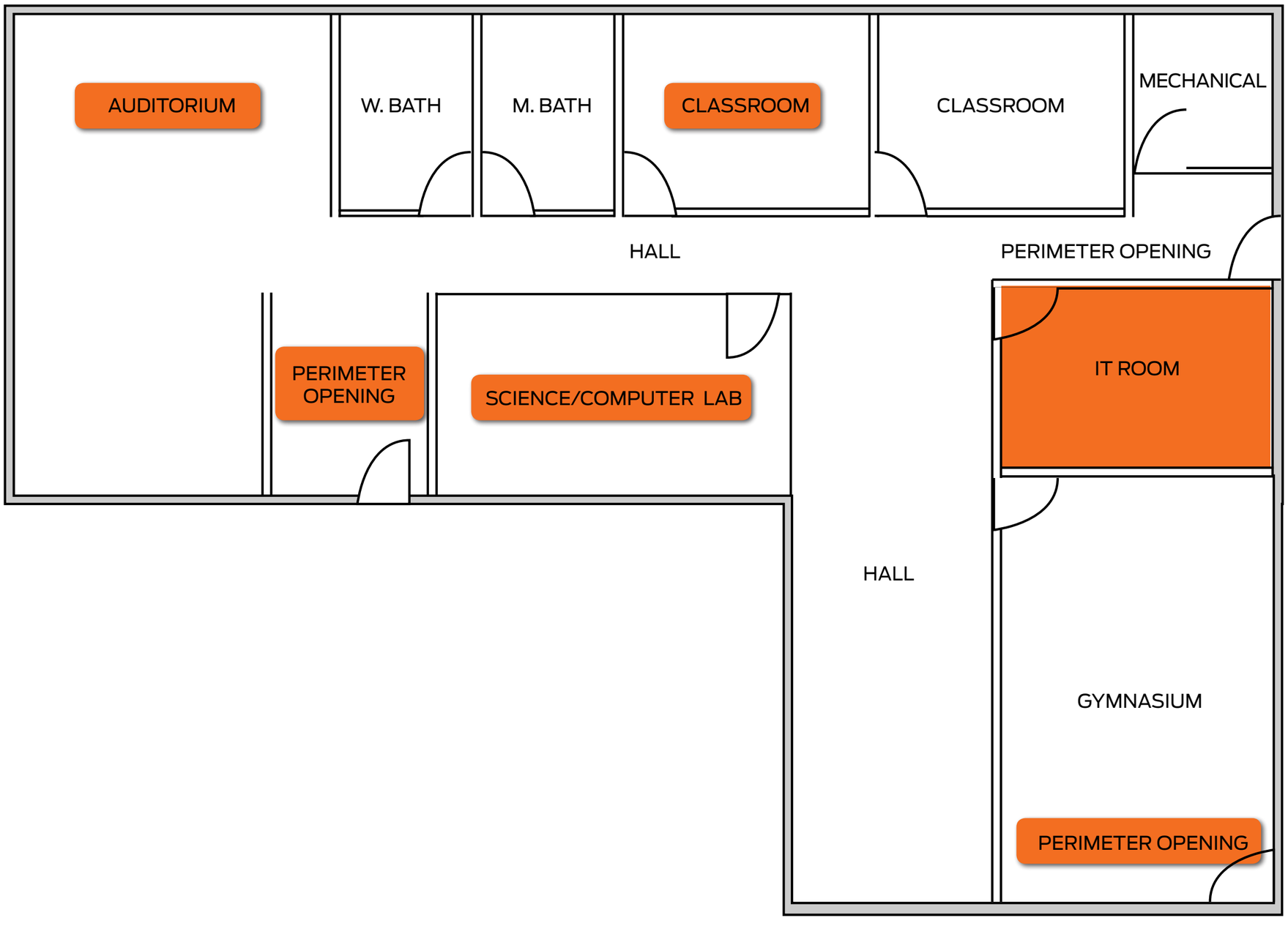




Education facilities

IT rooms

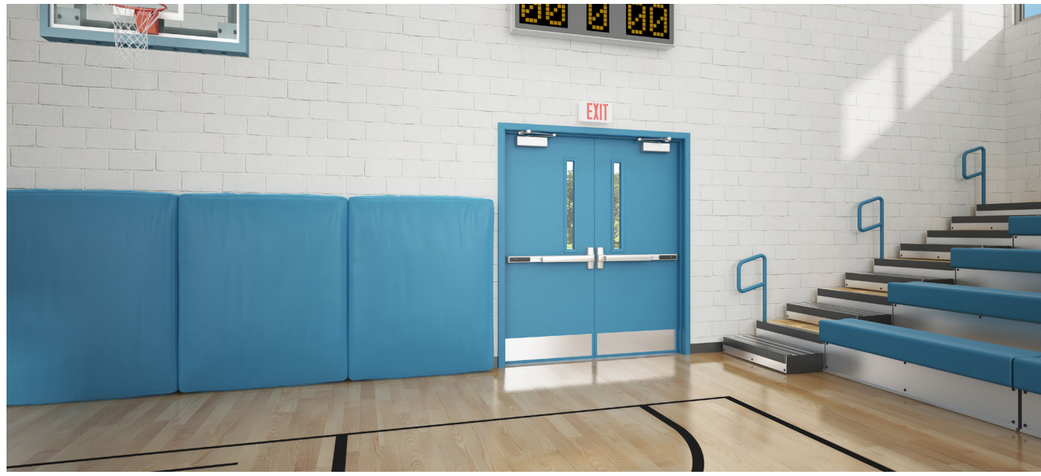
IT rooms, such as data closets or server rooms, contain sensitive information and expensive equipment. Wireless solutions make it convenient to control and monitor access to these spaces, which often need greater security than conference rooms and are only accessible by a small group. Real-time visibility provides reference of who request access to the room and when.

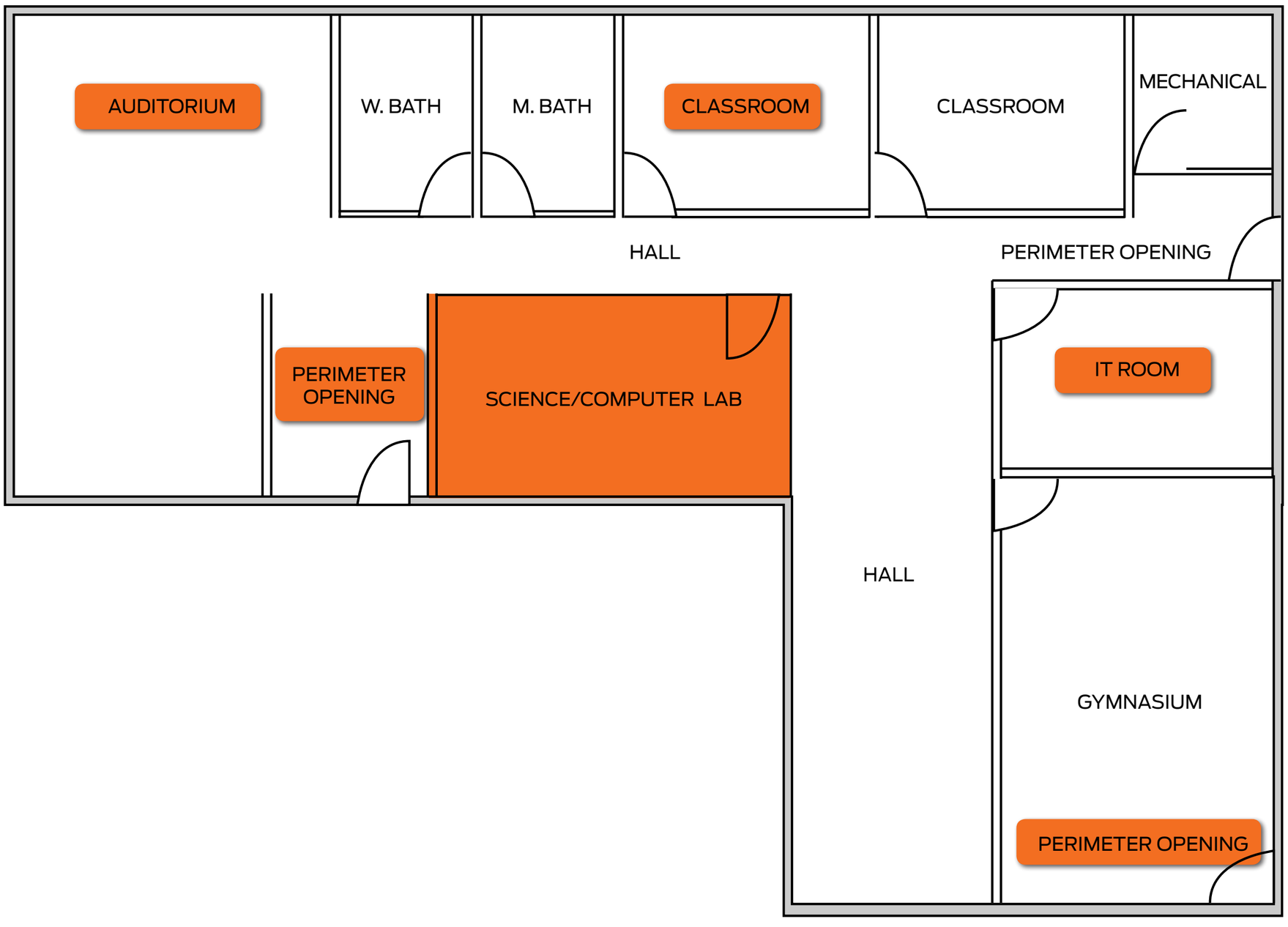


Education facilities

Science laboratories and computer rooms

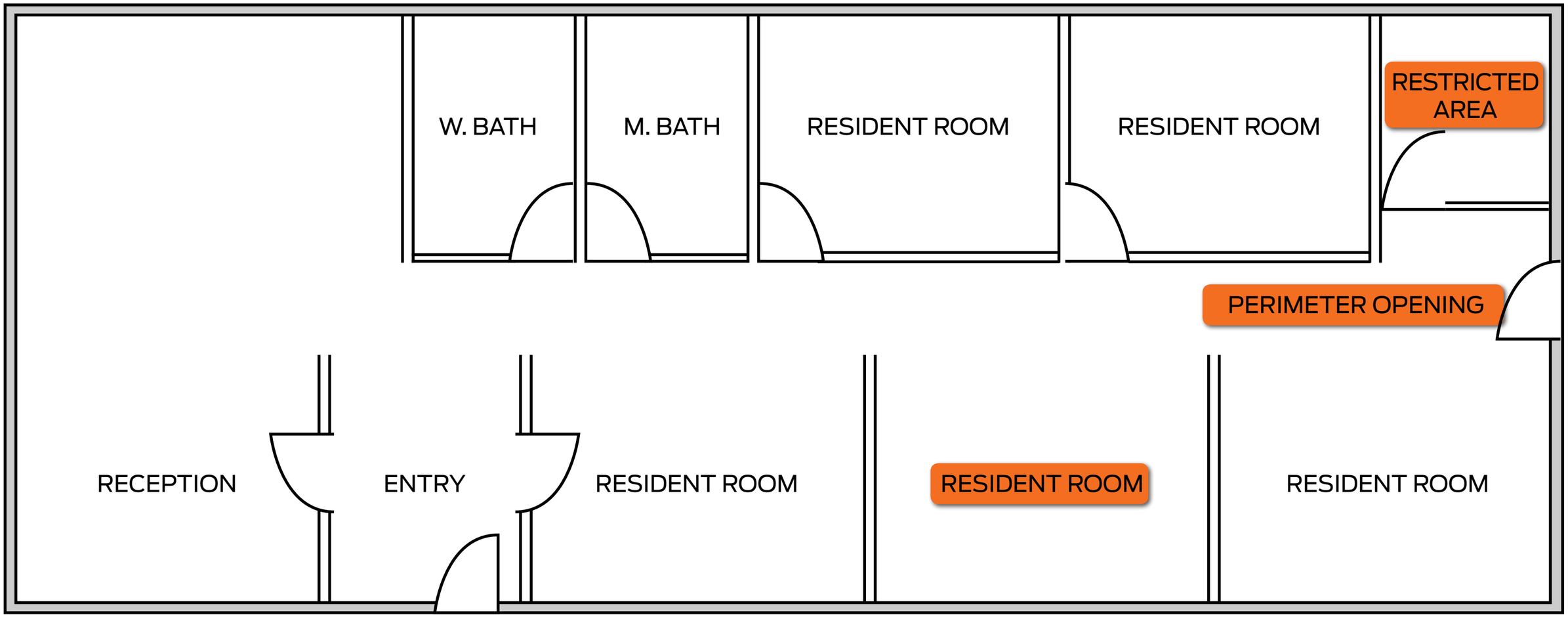
Access to spaces like laboratories and chemistry or computer rooms may be limited to specific faculty or based on specific schedules for students. These spaces contain valuable assets or hazardous materials that require protection. Because these areas and assets are intentionally controlled, it is important to know who accesses a space and when. Electronic access control mitigates risks associated with lost or stolen keys and provides detailed audit trails and real-time data that's not available with mechanical solutions.





Assisted living facilities

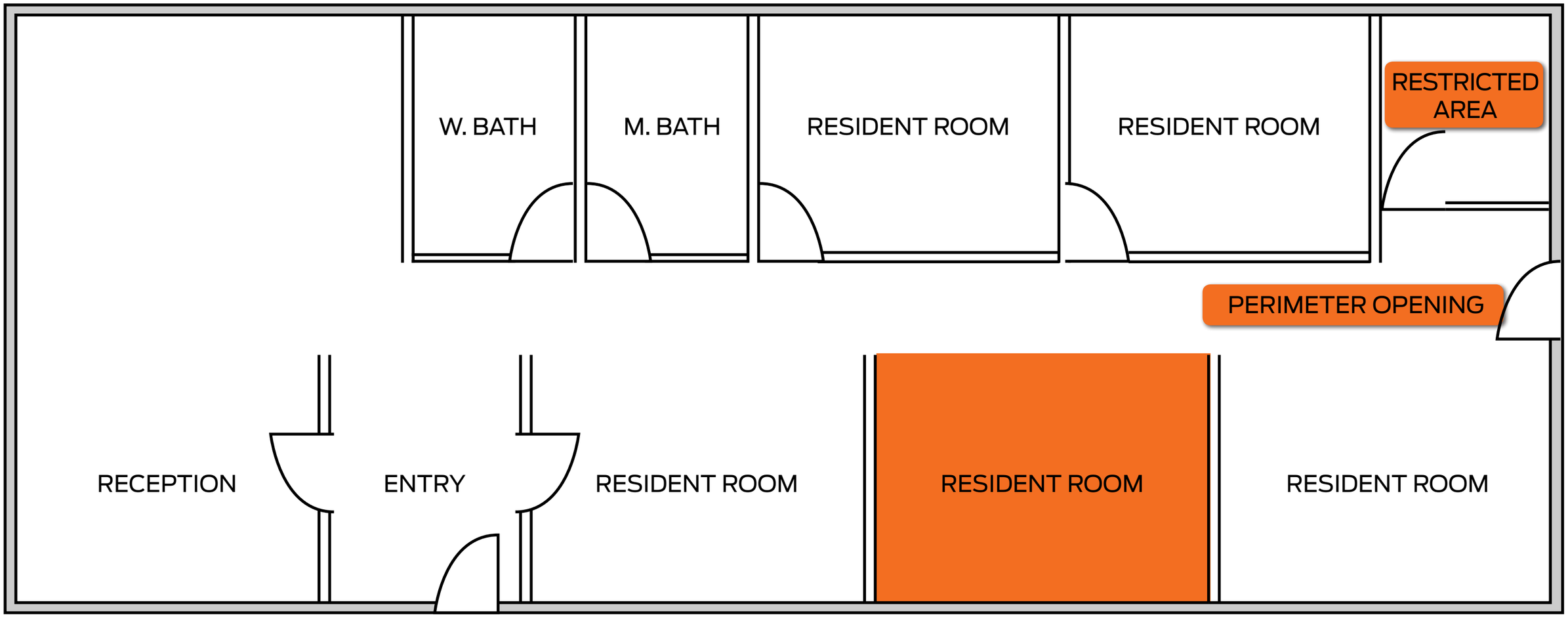
Assisted living facilities must blend security in a way that protects its residents, employees and visitors while encouraging freedom of movement amongst residents. From perimeter doors to medical records and pharmacy rooms—every area has unique requirements. Managing the wide range of medical, residential and business needs can be challenging. The application of electronic access control can simplify the coordination of these needs while enhancing the experience for residents and employees. It's common for the front and rear entrances to have electronic access control, but there are benefits beyond the main doors.



Assisted living facilities

Resident rooms

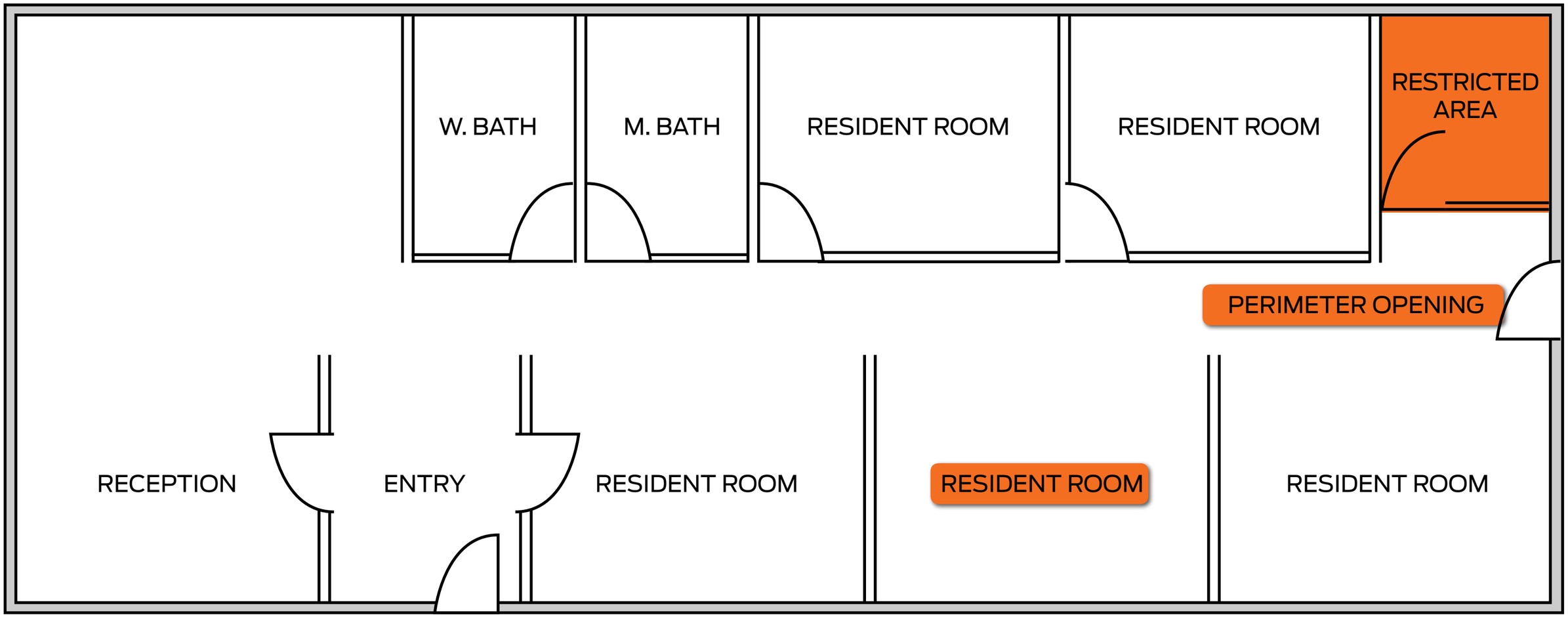
The use of mechanical keys can be challenging to residents who easily misplace their belongings or have trouble with the mechanical operation of locking their rooms. For staff, wireless electronic access control overcomes the challenges of managing lost keys. Additionally, electronic credentials offer a pleasant, ergonomic user experience.



Assisted living facilities

Restricted areas

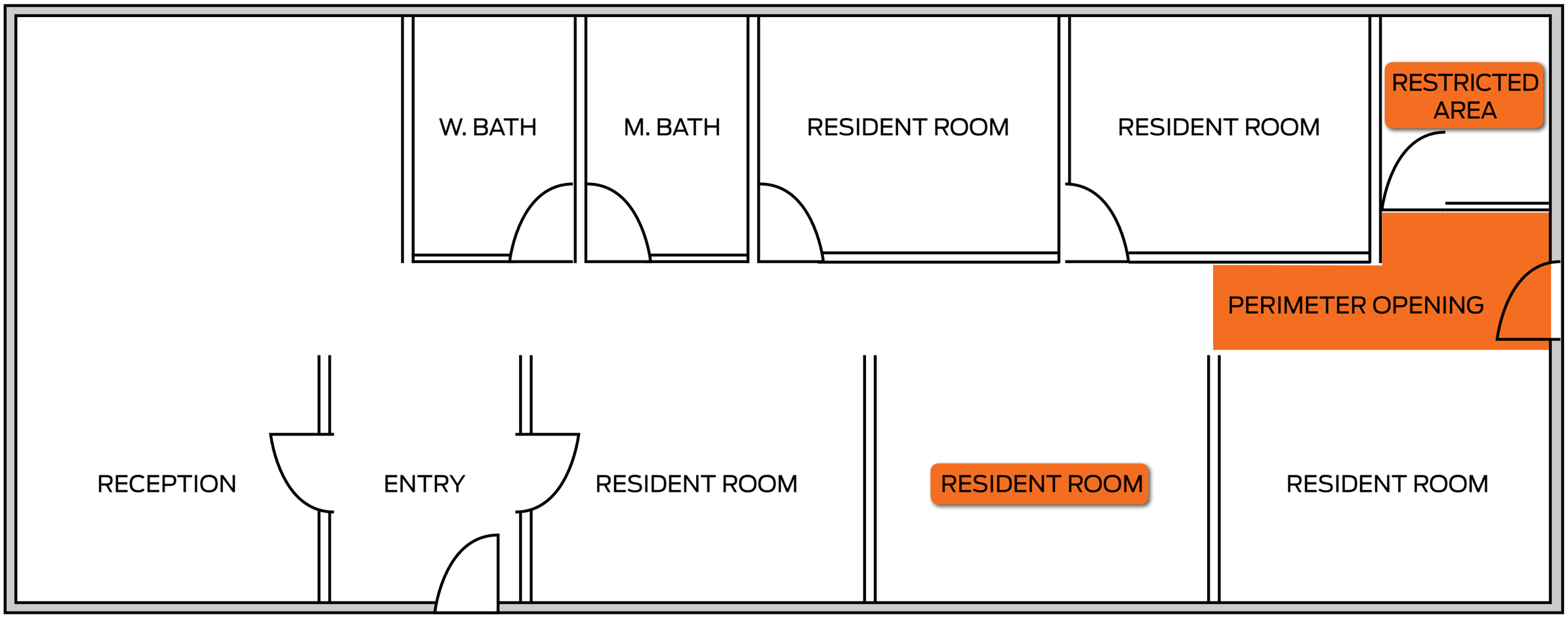
A select group of medical personnel is granted access to high-security areas like the pharmacy, IT rooms or storage closets. Resident records, pharmaceuticals and other sensitive assets are stored in these spaces, so it's important to know who accesses a space and when. Electronic access control mitigates risks associated with lost or stolen keys and provides detailed audit trails and real-time data that's not available with mechanical solutions.



Assisted living facilities

Secondary openings

While primary openings are typically monitored and accessed electronically, there are additional secondary access points around the building that need to be considered. Historically, mechanical solutions are implemented on these openings due to the cost of electronic options. Wireless monitoring and access control solutions enhance the security of these access points, while enabling staff and patients to enter spaces using the same credential as the rest of the building, including resident rooms.



Hear from your peers

Industry professionals share their experience with wireless electronic access control. Read how it has impacted their business and their customers.

Understanding the value of wireless access control for your customer

The evolution of wireless access control in the industry

Ease of adoption and lower procurement costs allow end users to control more openings

Wireless access control unlocks new opportunities for integrators

Understanding the value of wireless access control for your customer

By Clayton Brewer, NextGen Security

> “Work with the end users to see what makes sense and what their traffic flow needs to be.”

Security integrators that take the time to establish strong, trusting relationships are likely to experience long-term business with their customers. Many customers look to their security integrator and service provider to be their trusted experts, understand their needs and present solutions that solve those needs.

Clayton Brewer, Northeast vice president at NextGen Security, understands the integrator-end user relationship is something to be valued. He believes it’s essential for integrators to provide customers with new, proven technology that is cost effective, easily implemented and accomplishes the end user’s security needs.

New technology

Everyone wants to offer end users the latest technology, but integrators first need to be sure the technology works the way it should and that it will fit with their customers’ demands. Brewer’s advice to any integrator that is going to deploy something is to ensure everyone is trained on the solution, from engineers to technicians to sales personnel.

“If someone is selling it, they need to understand the product and how its designed,” he says. “Once you sell it, the engineers and technicians need to understand how to deploy it. If not, that’s the fastest way an integrator can put a bad taste in a customer’s mouth with a new product.”

When it comes to wireless solutions, there are often misconceptions about the stability and reliability.

“A lot of times clients think wireless locks are Wi-Fi, but in reality, it’s two different solutions and technologies,” Brewer says. “With a Wi-Fi lock, it’s only as stable as the network. But with wireless, we’ve been happy with the ability to eliminate cable, be more efficient for the customer in terms of deployment and provide that level of stability that a hardwired door has. We present that to our customers. They’re still going to have that same quality and reliability but it’s more cost effective.”

It’s also important to ensure the solution fits the client’s specific needs.

“Your wireless lock technology is not for every door. At a main entrance with high volume traffic, they probably want a hardwired door. But for certain applications, like a residence hall where they’ve got 100 suites in there, it’s a great solution. Work with the end users to see what makes sense and what their traffic flow needs to be. It’s not just here is a product we think will work, we’ve got to understand how they want it to be managed, then we can figure it out from there.”

Ease of deployment

NextGen Security recently worked on a university project where there were several older buildings, many of which had student suites. The university wanted to install wireless standalone locks on all of their residence hall doors. According to Brewer, they wanted to understand traffic patterns and the ability to pull reports. The goal was to find a solution that gave the university this greater control over their residence halls with the access control system that they were already comfortable using. They didn’t want a separate system to have to manage.

“Allegion locks can work with a lot of different access control systems out there” says Brewer. “A lot of clients don’t want to deal with another system on their network or another standalone product. Being able to integrate with what they have is another big selling point.”

Another challenge was aesthetics due to the age of the buildings. “A lot of them are cement blocks,” Brewer says. “Running cable was very difficult and they wanted to stay away from conduit. A lot of these location would have required that. When you start adding conduit, it increases costs.”

Next Gen Security wanted to maximize the solution for the campus and achieve their goal of putting electronic access control on each suite door, so they needed a more cost-effective solution. Brewer and his team installed Schlage® AD-400 wireless locks on every door in a phased approach, going building by building. The locks work with the same cards the school issues students, so it was a simple transition.

Cost savings

Eliminating the need to run wires was a huge savings for the university. Brewer emphasizes the importance of presenting cost-effective solutions to customers. He says that while many see a lock as a lock, cost is what the customer sees. If integrators can eliminate costs by not having to run all of the cables they normally would, and the doors still function with all of the expected features, they’ve got a win-win product.

The evolution of wireless access control in the industry

By Howard Hutchinson, Allied Universal

> “Instead of it being simply a point of entry and a point of exit, the idea is truly to control access to any location.”

Howard Hutchinson, senior director of sales at Allied Universal, was born and raised in the security industry and has witnessed the evolution of wireless access control firsthand. He recalls when many believed if you couldn’t put a wire to it, it wasn’t a solution.

That said, Hutchinson has seen this mindset shift during the last five years. “Technology has improved and many of the initial issues with loss of transmission and security have been rectified. As we know, there isn’t much in today’s environment that cannot be accomplished wirelessly.”

One of the biggest trends Hutchinson has noticed is that customers have begun to look at what access control is truly designed to do.

“Before the points that were being protected by access control were often limited based on availability, cost and technology. Instead of it being simply a point of entry and a point of exit, the idea is truly to control access to any location. Once end users begin to understand that as a concept, they are more in tune with how to protect their facility.”

Client needs: Beyond main entrances

As wireless solutions have evolved, the applications have expanded. Access control is no longer limited to exterior doors. And as Hutchinson said, many are realizing the full potential of wireless solutions. To help customers identify applications, he recommends asking clients about the areas that concern them most. For example, the Allied Universal sales team visited five hospitals in the Carolinas. Almost all five said they were concerned about the security of their human resource departments.

“We’ve found that they are trying to protect their human resources and their financial departments, which are often overlooked because of budgetary reasons. Before they were more concerned with protecting main points of access versus some of their most valuable resources—which are people. A lot of organizations have issues with individuals getting into the wrong doors and seeing the wrong people. Now they are trying to lock those doors for their HR staff.”

Another good example is religious facilities. Recent events have led many to review their safety and security protocols so that the facility and those who attend are not in jeopardy. Hutchinson says they are controlling access to secure rooms and day cares that previously went without access control due to costs. Now they are able to implement wireless access control to protect their assets at hand.

“Wireless solutions have dramatically improved our industry,” Hutchinson says. “They have assisted our clients in getting the technology where it needs to be. Oftentimes, there is no other way.”

Ease of adoption and lower procurement costs allow end users to control more openings

By David and Mike Mims, Georgia-Florida Alarm

“In a building that is 25 years old, there is no telling how many keys they have out to those locks. In essence, they have no audit trails; they have no security on the doors.”

Georgia-Florida Burglar Alarm Company president, David Mims, and vice president, Mike Mims, have found that electronic access control has become increasingly more prevalent during the last decade. In fact, they say in most cases, their customers request electronic options.

“It’s not like 10 or 15 years ago when there wasn’t a lot of access control around so people didn’t know about it,” says David. “They’ve already realized they need to move in that direction. Once they contact us, it’s ‘This is what we want, now how do we get there?’”

Expanding opportunities for access control

Wireless solutions have opened new possibilities for the industry, and Georgia-Florida Alarm are among those who have seen the benefits of adopting the technology. Now that the customers are demanding these solutions, security integrators like David and Mike are positioned to introduce new applications that are a good fit for the wireless technology.

For example, they recommend commercial facilities consider wireless solutions for server rooms or sensitive storage areas. In healthcare facilities, anyplace where identification information or medical records are kept should be under audit. Therefore, it’s best to have access control on those openings.

“K-12 schools are starting to secure main office records, as well,” says Mike. “And they typically have access control where they have audio visual or expensive equipment stored. Even band instruments and computers, they lock them down. They need the audit ability.”

Ease of adoption

Wireless solutions are less expensive, which allow end users to adopt electronic access control on more doors. Plus, installing these devices causes less disruption to the building. This is especially true in retrofit situations where pulling wire and drilling holes can become costly and leave the openings disfigured.

“In the arena we work in, which is mostly state departments, they’re changing offices all the time,” says David. “In the wired world, we’re moving wires, pulling it out and trying to fill up a strike hole. Or we’re leaving the strike behind and going to another door altogether. With wireless, we’re just taking off a door knob, going somewhere else and putting back on and we’re done.”

“We just completed a project with about 20 Schlage® NDE wireless locks, which was a state of Florida government job,” David adds. “It had an old wired system in there and we replaced it with the NDE locks so we wouldn’t have to rewire the system. It was a much quicker and cleaner installation.”

Security and convenience

David says, “In a building that is 25 years old, there is no telling how many keys they have out to those locks. In essence, they have no audit trails; they have no security on the doors. With access control, they know who is coming and going through the doors. They can immediately control who can and cannot come through the door. And it’s more convenient than toting around 500 keys.”

Wireless solutions conveniently enhance security for end users. David notes that key management is much simpler and more secure because end users have greater control over their access rights. If an employee is terminated at 5 p.m., they can immediately deactivate that credential in the system. Beyond key management, building automation can start to simplify daily routines. The access control system will lock down a building at night and unlock it in the morning. And with wireless devices on interior doors, the entire facility is more secure.

Business impact

Overall, end users are interested in wireless solutions and the value these add. The ease of adoption and lower costs has allowed customers to add wireless solutions to more openings, which in turn has provided new opportunities for Georgia-Florida Alarm.

The popularity of wireless solutions is expected to continue. Security integrators who embrace wireless technologies will be able to meet client demands and see continued business success.

Wireless access control unlocks new opportunities for integrators

By Adam Heiks, GenX Security Solutions

> “Once service starts, they can secure the property without having to manually run someone around the property.”

Greater adoption of wireless electronic access control has unlocked new opportunities for security integrators that weren’t possible with hardwired options. Wireless devices are flexible and easy to introduce, which means end users can add access control to a greater number of doors—even those that were once out of reach.

This introduces new business opportunities for security integrators. It’s true that wireless allows end users to connect more doors, which means more points of service opportunities. But it also allows them to secure openings that they couldn’t physically get to before. Simply put by Adam Heiks, owner of Gen X Security Solutions, “Wireless opens doors to new doors.”

A secure sanctuary

For example, Heiks recently worked on a 100-year-old church building with circular ceilings. It was part of a campus that also had a few newer, separated buildings. To secure the premises, the staff had to manually lock each opening during and after service.

“They couldn’t keep people from wandering,” Heiks explains. “They would be in the middle of service and people would be walking in asking for help. Then it became pretty scary because they had people ending up in the day care.”

Everyone came to the consensus that they needed security and the ability to lock down the building. But they had to find a way to balance that with the openness that churches offer to the public.

He adds, “Being so old, they wanted to keep everything looking similar, so the biggest issue became the aesthetics. Without using wireless, I couldn’t begin to tell you how we would have done it without making a huge mess of those circular ceilings.”

“At the office building we made a visitor’s section where people can come up and ring the bell,” Heiks says. “They have someone in the center building that watches what is going on around all the buildings and have a single button that can lock the facility. We did video, access control and network for them. They are open to the public during certain amounts of time, then the doors lock automatically behind them or they can lock it down. Once service starts, they can secure the property without having to manually run someone around the property.”

Expanding access control

In addition to enhanced security and convenience, Heiks has found the ease of deployment and aesthetics to be appealing to end users. “Customers are definitely open to anything that’s going to keep the building looking the way they want,” he says. “A lot of what we do when running wires is disturb the property. You’re not distributing as much property with wireless. It looks much more professional.”

Eliminating the need for wires allows security integrators to connect doors that were once off limits. Wireless solutions overcome those issues to enhance security on interior doors. More connected doors are a benefit for both the end user and the integrator.

Wireless solutions enable you to enhance the end-user experience by improving security, operational efficiencies and convenience for your customers. We hope you find this resource helpful and encourage you to utilize the information as you communicate the value to your customers. To dive further into the topic of wireless or ask questions, contact your Allegion representative.

About Allegion

Allegion (NYSE: ALLE) is a global pioneer in safety and security, with leading brands like CISA®, Interflex®, LCN®, Schlage®, SimonsVoss® and Von Duprin®. Focusing on security around the door and adjacent areas, Allegion produces a range of solutions for homes, businesses, schools and other institutions. Allegion is a $2 billion company, with products sold in almost 130 countries.

For more, visit **www.allegion.com.**

KRYPTONITE ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

013061, Rev. 03/19
www.allegion.com/us

ALLEGION™