# FUTURE FOCUS: HOW OUTDATED ACCESS TECHNOLOGY HURTS YOUR MULTIFAMILY OPERATION

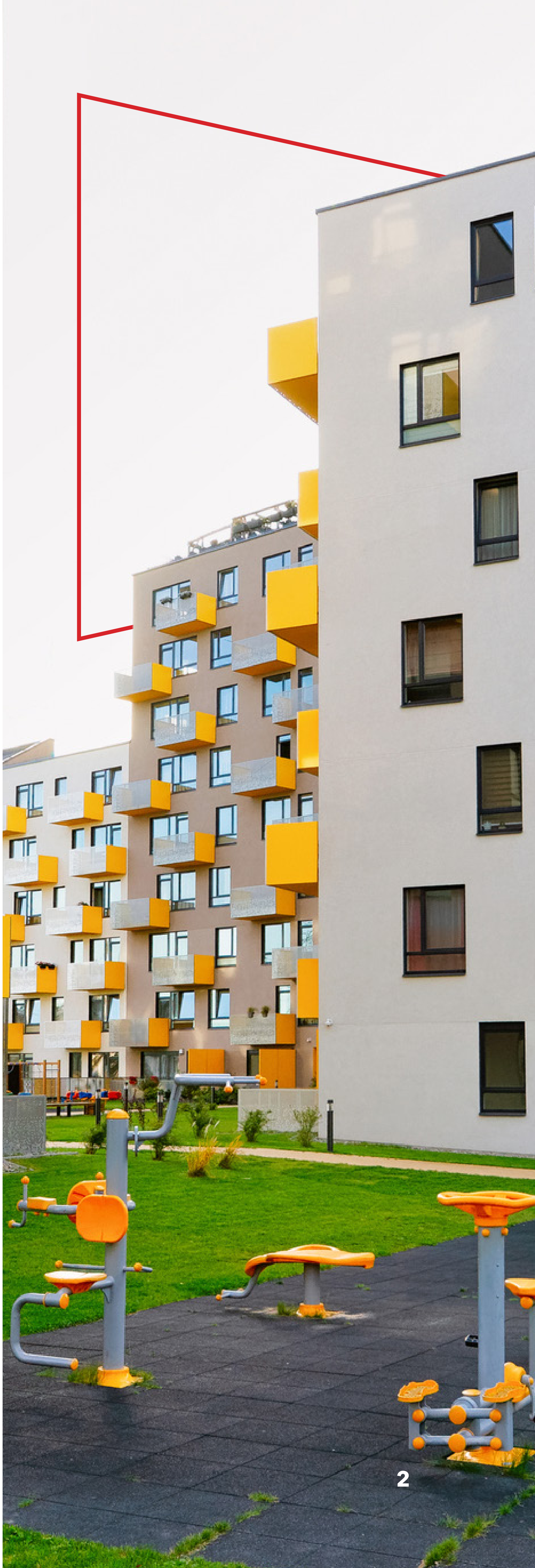
KASTLE

## Is your multifamily building's access control system working for you or against you?

The challenges that owners and managers of multifamily properties currently face are different than they were even two or three short years ago. Even though rental prices increased in most metropolitan areas in 2022, and occupancy rates remain high, tenants expect growing numbers of amenities. At the same time, costs for ongoing maintenance and upkeep have skyrocketed with rising inflation.

In inflation-adjusted terms, operational costs for multifamily properties are higher than they've been in decades, making it harder to maintain profitability. In addition, the real estate market faces the triple threat of high-interest rates, inflation, and possible recession. Against this backdrop, it's more important than ever for on-site management teams to cultivate efficiencies that can save time, reduce labor costs and preserve net operating income (NOI).

However, far too many multifamily properties—even fairly new construction that incorporates more modern technology—rely on an outdated operating model in which processes and systems exist within silos, all run independently by the on-site property management staff. Many property owners and managers find that they're losing an unseen battle with hidden operational costs due to the inefficiencies inherent to this model, and these inefficiencies are ultimately eroding the profitability of their investments. Often, they also find themselves overextended as they struggle to keep properties up to the standard that their residents expect.



One critical core operational function is managing property-wide access and security for the staff and residents of a multifamily community. Secure access is something that property owners and managers are expected to deliver to their residents, but all too often this function is considered a utilitarian afterthought.

For their access control systems to maintain reliable operations, property owners and management teams often need to invest more attention and expertise into them than they're prepared for. And if they don't do it themselves, they spend valuable time identifying a vendor to take responsibility for the system, which comes with its own host of issues. Would that vendor be the manufacturer? The distributor? The installer? If someone's hired to maintain a system, how does a property manager gauge whether the job is being done well?

Consequently, property managers are left with less time to do the functions that they've been trained to perform—things like marketing unoccupied units, conducting tours for prospective residents, and completing other revenue-enhancing activities. In other words, the inefficiencies and complexities of their access control systems are pulling them away from what they do best (and, often, where their expertise is needed the most).

The end result is that inefficient access control strategies are driving overall inefficiencies in property management, compromising the quality of residents' experience, and contributing to higher vacancy rates and elevated operational expenses. It doesn't have to be this way.

# PAINFUL SYMPTOMS OF AN OUTDATED ACCESS CONTROL STRATEGY **(FOR PROPERTY MANAGERS)**

Ensuring that residential communities are operating efficiently—and that tenants' needs are being met—lies at the heart of a multifamily property manager's professional responsibilities. Tenants must be able to access their units easily and the property must be secured against intruders. This means that property managers are tasked with supporting multiple access control functions.

## THESE ESSENTIAL ACCESS CONTROL FUNCTIONS INCLUDE:

- **Credential management**. The person who is responsible for the access control system must keep track of an ever-changing roster of residents and maintain the database where their profile information is stored.

- **Hardware maintenance.** Access control systems are typically comprised of an array of card readers and video cameras, and these devices will remain operational only if they're taken care of properly.

- **Staff training**. On-site staff members must understand how to operate the access management system and video surveillance systems that are in use on the property. In the current labor market, where turnover rates are high, these staff members will need ongoing training, especially as new hires come on board.

- **Data management.** All resident profiles, records of access activities, and video recordings will need to be stored so that they are both secure and accessible (in case the information is ever needed by law enforcement or for other purposes).

- **Security monitoring.** Unless someone's watching over it, a security system can't protect residents and the property. Monitoring the system may entail hiring—and supervising—expensive guards, monitoring alarms or keeping an eye on video surveillance systems yourself, and keeping track of issues and resident violations.

- **System integration**. In the long run, the entire property will operate more efficiently if access control systems are linked with elevator operations, video intercom systems, amenity access control, and parking management systems. Of course, it's also possible to run all of these systems separately, but doing so is labor-intensive and inefficient.

- **Software upgrades.** Access control systems should have regular software updates to ensure their resilience against the latest cyber and physical security threats. This also ensures that they'll keep performing as well as possible, even as residents' requirements evolve.

Multifamily property managers are highly skilled individuals who are accustomed to wearing lots of different hats. Nonetheless, they're usually not experts in database management or security system surveillance. And they're busy. They don't have extra time to waste on access control system management, and thus often achieve less-than-excellent results. Because access control isn't their main area of focus, they're left to trust their instincts when making decisions about these systems. Or, they'll rely on whatever vendors tell them, with no guarantee that they're getting best-in-class advice.

Most access control system vendors don't offer long-term service contracts. They're typically called in on an ad hoc basis when things go wrong, so they don't have a longstanding commitment to making sure that things will function well over time. In most of these relationships, access control system vendors don't have a sense of ownership over the quality of service they provide.

Because this sense of vendor obligation is absent, and because relationships are often short-term, staff members rarely understand the historical context of events that take place at a particular property. Instead, each staff member must learn about an individual system's operational background and maintenance history again. Because churn rates are currently so high for on-site staff, few will recall previous events or past maintenance activities. When the vendor's attention isn't dedicated to your individual property, there's no shared knowledge base, and no one to take ownership of building out maintenance plans for the future.

The events of the past few years have compounded the challenges that property managers face. Because more residents are now working from home, they're more likely to call for service or support during the day. This means that property managers have less downtime than ever, leaving them less able to catch up on ongoing access control system maintenance tasks.

# PAINFUL SYMPTOMS OF AN OUTDATED ACCESS CONTROL STRATEGY **FOR PROPERTY OWNERS AND ASSET MANAGERS**

Although access control might seem like a commodity service that's necessary to provide to tenants, implementing the right access control strategy—one that's modern and efficient—can streamline operations in ways that preserve consistent income streams and ensure return on investment.

An outdated access control strategy will leave your team in endless service recovery mode, with unhappy tenants frequently complaining about systems that don't work as they should. This means you'll face ongoing expenses for repairs, you'll need to apologize to tenants, and you may even want to offer rent rebates to make up for the ways that the service quality has fallen short. You'll also have to communicate with tenants about systems that are down, and this ongoing "downtime" messaging does the opposite of highlighting the benefits of living in your property.

Weak on-site security can increase operational costs as well. If staff can't keep up with system surveillance, theft, vandalism or abuse of the property make take place during the gaps in monitoring. Not only does petty crime have the potential to harm your tenants directly, but it can quickly lead to reputational damage. If residents post on social media or online review sites that their packages are getting stolen instead of delivered, this can do immediate harm to your retention and marketing efforts.

Ultimately, if the property falls into disrepair because you can't escape from recovery mode, you may even need to reduce rents or offer other concessions to attract residents. This will further reduce your revenues and squeeze NOI.

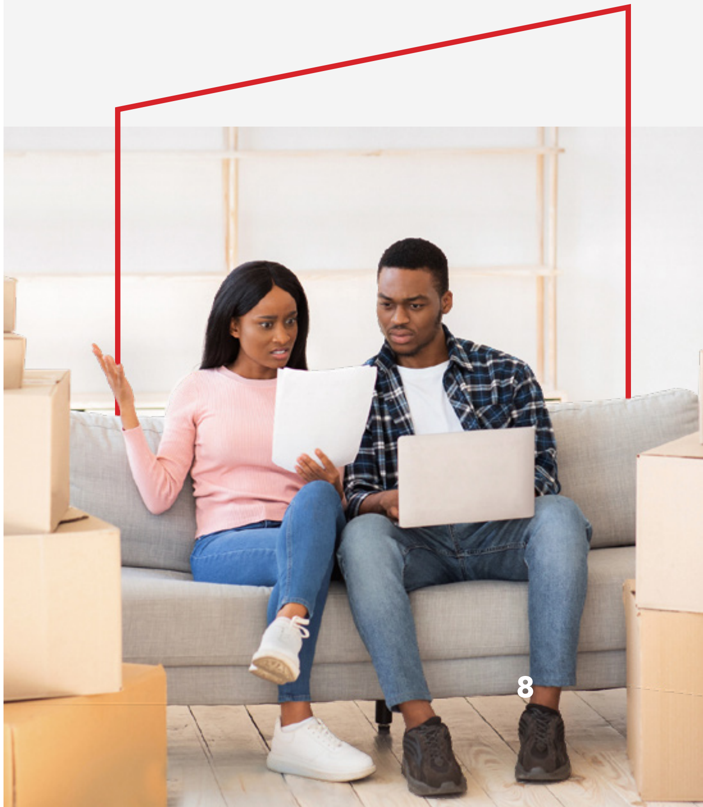
If staff are spending much of their time reacting to problems and fixing things that have broken, they'll be less available to market the property. Even if you increase your advertising spend to address the churn that inevitably occurs when systems aren't working as they should be, property managers will have less time to spend with the prospective tenants who show up at the property. The longer-term results include elevated advertising costs and higher vacancy rates.

For the business, the longer-term outcomes can be unpleasant. While an outdated access control strategy can lead to higher-than-expected operating costs, it can be difficult to pinpoint exactly what's gone wrong because so many aspects of your operations can be tied to access control system failures. This means it's challenging to figure out which problems to address first. In addition, because your on-site staff aren't experts in operating and maintaining these systems, you may not know that they need ongoing upkeep. This can lead to higher maintenance and repair costs on a long-term basis, as well as expensive service calls that take place after hours or on the weekend.

The reality is that an ad hoc approach to access control and security cannot protect your budget, time, or the value of your assets. It opens a large number of often unforeseen financial and operational risks.

## THE BUSINESS COSTS OF THE WRONG ACCESS CONTROL STRATEGY:

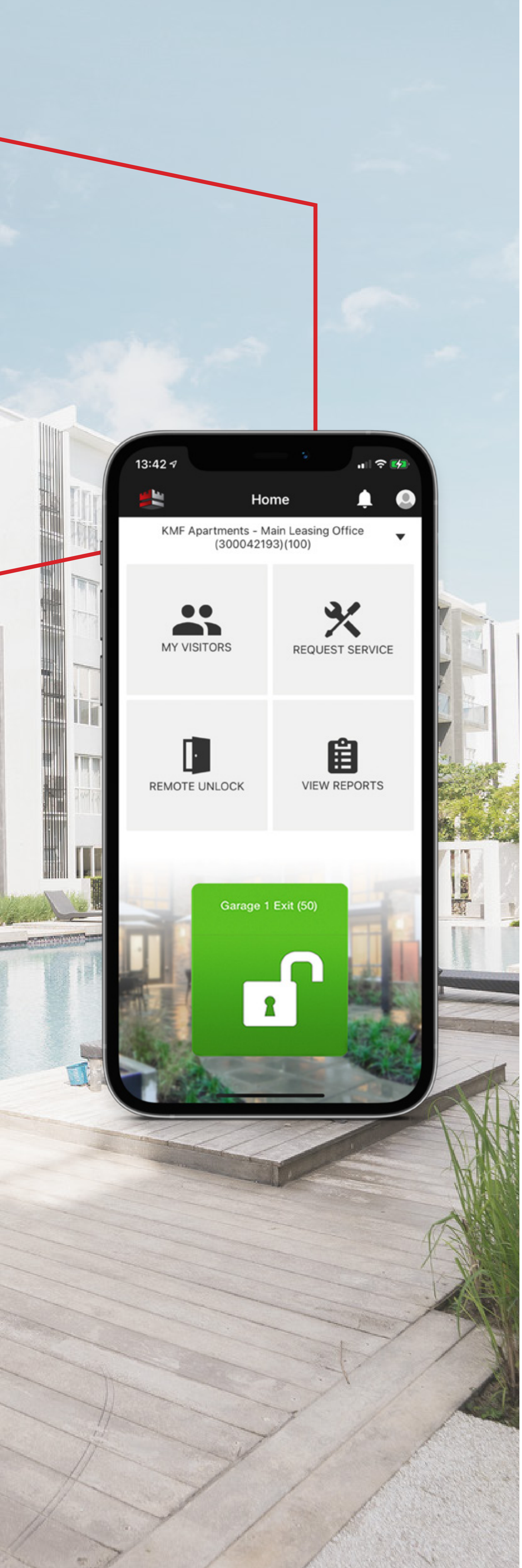
- Excessive operational expenses
- Frequent need for repairs to and replacement of systems
- Elevated maintenance and repair costs
- High-priced emergency service calls
- Unhappy tenants
- Tenant turnover
- Damage to your property's reputation and difficulty attracting new tenants



# RISING TO THE CHALLENGE: A BETTER WAY OF MANAGING YOUR ACCESS CONTROL AND SECURITY TECHNOLOGIES

When a particular operational function is critical to the success of your business but isn't where your core expertise lies, outsourcing that function to a professional provider who is specialized in that area often makes sense. This model has become particularly popular for IT and technology management. As businesses across industries have become increasingly data-driven and dependent upon digital technologies to achieve a competitive advantage, smaller ones are increasingly turning to managed IT service providers. For companies that aren't big enough to have dedicated in-house IT departments capable of managing all aspects of technology-related operations, managed service providers (MSPs) offer access to professional-caliber expertise at a tiny fraction of the cost of hiring dedicated in-house staff.

When you pursue a "managed services" approach, you're outsourcing a key aspect of your operations to be performed by dedicated experts in the area. In the case of IT services, this means that every aspect of your technology environment—from server management and hardware maintenance to cybersecurity and user directory management—will be run by a team of professionals with extensive expertise.



Whether you're applying it to access control and building security or any other area of your operations, this approach brings a plethora of benefits.

You'll always have access to the latest technology, with systems that are custom-tailored to your unique needs (and those of your residents). Not only will the staff tasked with managing these systems be experts, but they'll be held accountable for its performance on an ongoing basis. This means they have a strong incentive to do their jobs well and to create efficiencies. They're also incentivized to keep up with the latest advances in technology, since newer software and systems are invariably more efficient, secure, and easy to operate.

Managed service providers typically offer contract engagements with a fixed monthly fee. There are never any budget surprises, since you pay them to deliver services that are designed to meet your business's needs and suit its scale. At the same time, you'll have access to world-class access control and security technologies, operated by a long-term partner who is committed to providing you with top-notch service. You'll never need to worry about system compatibility or integration with existing in-building technologies, since your partner will take care of all of these things for you.

Engaging with a managed security service provider can actually add value to your asset. Their systems will integrate seamlessly with existing property infrastructure and technologies, so that you can make the most of what's already on-site. The provider will take full responsibility for the system's operations, so you'll never need to spend time and energy fixing things that don't work. This model also futureproofs your investment, since the provider will bring—and adapt your systems to incorporate—the latest technologies and developments in the field. The fixed-fee billing model supports consistent NOI.

In addition, a managed security service provider will ensure that your staff are no longer wasting time on tasks that are outside their core areas of expertise. Security system troubleshooting will be left to experts, who can proactively prevent issues that would have otherwise been costly and time-consuming. Their expertise will reduce the prevalence of error in all areas of system operations—from data entry to maintenance and monitoring. These experts will also be available to train your team to work with the system, making it easier for them and freeing their time for what they do best: marketing the property, welcoming prospective residents, and engaging with current residents to strengthen the community.

## BENEFITS OF THE MANAGED SECURITY SERVICES APPROACH

**Fewer Hard Costs:**

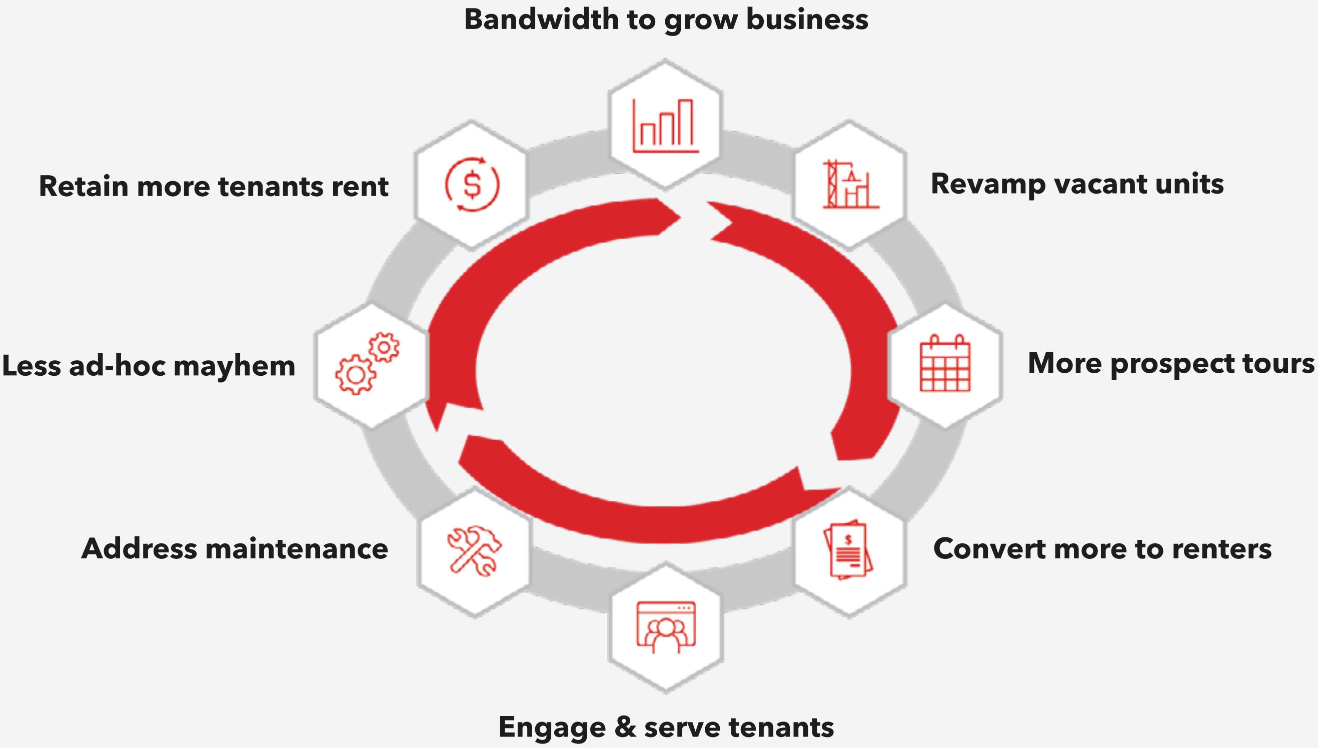
- No unplanned maintenance costs
- No hardware replacement costs
- No software upgrade costs

**Fewer Soft Costs:**

- No overhead lost on zero-value troubleshooting
- No need for added security headcount
- Less resident churn
- Reduced need for marketing spend

Ultimately, engaging with a managed security service provider can set in motion a virtuous cycle of continuous improvement. When on-site staff and property managers have more time to spend on marketing and improving the property, they'll be able to conduct more tours for prospective residents, converting more to renters. They'll also have more time available for engaging and serving tenants, and by better meeting their needs, they'll be able retain residents longer. They'll spend less time solving problems and fixing systems that are broken, and more time improving the residents' experience and building the community. In the end, this will lead to fewer vacancies, creating space to grow the business and improve its profitability.

## BUSINESS GROWTH CYCLE OF MANAGED ACCESS TECHNOLOGY



# ABOUT **KASTLE SYSTEMS**

We're an industry-leading managed security service provider that's dedicated to creating secure spaces and distinctive experiences by incorporating smarter technologies into the built environment. We have extensive experience customizing solutions for multifamily buildings, operating more hundreds of access control systems in residential properties nationwide, processing thousands of residents and their visitors across the nation.

As the first company to offer access control and security services according to the security-as-a-service model, we're proud of our expertise in bringing together cutting-edge technology and real estate business acumen. Our open integration approach makes it easy to work with your existing systems, and we have thousands of satisfied customers across a broad array of industries. We've consistently achieved the industry's best J.D. Power ratings across millions of users, and our average customer stays with us for nearly a dozen years.

**Kastle**

The leading tech-enabled Real Estate operating platform providing services to Commercial Real Estate, Enterprises, Multifamily

**2,500** Buildings

**47,000** Businesses

**1.8 Million** Users

**4 Million** Visitors

***700+ and 250+ Local Employees within 20 min. of National Landing***

Select Customers

3rd Party Validated World-Class Service

Best Places to Work

CapitalShield Public-Private Partnership

KASTLE

HEADQUARTERS
6402 Arlington Boulevard
Falls Church, VA 22042

855.527.8531
info@kastle.com

License Number DCJS #11-2295

www.kastle.com