# Why Locks Are Losing Ground

## Idea In Short

Physical security has shifted from a hardware problem into a data problem, and organisations still running on mechanical keys are the ones most exposed by that shift. A lost key can force a full rekeying of every affected door, with no reliable record of who used which entry point or when, while a digital credential can simply be switched off the moment a phone goes missing. Cloud-based platforms now let administrators manage permissions across multiple sites from a single screen, covering everything from student housing to construction sites to outdoor assets like gates and containers. The decision facing most organisations is no longer whether to move away from mechanical locks, but how to sequence that move, starting with the highest-risk entry points, choosing open standards over a single vendor, and building in the data protection policies that digital access logs now require under rules like the GDPR.

Physical security has changed more in the last decade than in the previous fifty years combined. Buildings that once relied on mechanical keys and manual logbooks now run on digital infrastructure that can be monitored, updated and controlled from almost anywhere. This shift is not just about convenience, it reflects a deeper rethink of how organisations manage risk and accountability.

## The Limitations of Mechanical Security

Mechanical locks have served buildings for centuries, but they come with inherent weaknesses that become more obvious as organisations grow. A lost key means every affected lock may need replacing, and there is rarely a reliable record of who used which door and when. For facilities managers overseeing multiple sites, this lack of visibility creates ongoing administrative burden and genuine security gaps.

Keys can also be duplicated without authorisation, and once that happens, there is no way to know how many copies exist or who holds them.1 Businesses handling sensitive data,

valuable stock or vulnerable occupants cannot afford that level of uncertainty. This is why many have started exploring digital alternatives that offer better control without sacrificing ease of use.

Master key systems compound this problem, since a single master key opens many doors at once, and losing one forces a far larger rekeying effort than losing a single-door key. Insurers increasingly factor in a facility's documented level of access control when underwriting liability coverage, which gives mechanical-only buildings a real financial disadvantage beyond the operational one. That documentation gap can also complicate insurance claims after a break-in, when carriers increasingly ask for evidence of who had access to a space before authorising a payout. The gap is especially visible after a security incident, when investigators need a precise record of entry and exit that a keyed lock was never designed to produce.

## How Digital Access Control Changes the Equation

Modern access systems replace static keys with credentials that can be issued, adjusted or revoked instantly. A lost phone or fob does not compromise the entire building, because that single credential can simply be switched off. Administrators gain a clear audit trail showing exactly who entered which space and at what time, which matters enormously for compliance and incident investigation.

Cloud based access control takes this further by allowing permissions to be managed remotely across multiple locations through a single platform. Instead of dispatching a technician to reprogram a lock on site, administrators can update access rights from a laptop or mobile device within seconds. This is particularly valuable for organisations with distributed properties, such as retail chains, housing associations or logistics companies, where coordinating physical visits to every site would be slow and costly. Demand for this kind of system is growing quickly across the wider industry, with the global access control market valued at over $10 billion in 2025 and projected to keep expanding at a high single-digit annual rate through the end of the decade.2

Energy efficiency is another underappreciated benefit. Many digital locking mechanisms require no external wiring and draw power only when in use, which simplifies installation considerably compared with traditional electronic systems that demand cabling throughout a building.

These systems also tend to integrate cleanly with other building technology, linking access events to video surveillance, visitor logs and alarm triggers so that a single incident can be reconstructed from multiple data sources rather than from memory alone. That level of integration was rarely practical with mechanical locks, since a key by itself carries no data and leaves no trace once it is returned to a pocket. Facilities teams managing several properties often cite this consolidated visibility as the single largest operational improvement over their previous setup.

### Common Use Cases Driving Adoption

- Shared housing and student accommodation, where tenants change frequently
- Construction sites requiring temporary, time-limited access for contractors
- Healthcare facilities needing strict control over medication storage areas
- Commercial offices transitioning to hybrid work schedules with variable occupancy

That last category has grown substantially on its own, as office utilization patterns have shifted year over year and property teams have had to rethink how access is provisioned for a workforce that is rarely in the building on a fixed schedule.3 Each of these settings shares a common thread, access needs that change too often or too unpredictably for a physical key to handle gracefully. Retail chains managing seasonal staff turnover and multi-tenant commercial buildings coordinating dozens of individual leaseholders fall into a similar pattern, where the volume of access changes alone makes a physical key system impractical to administer well.

Outdoor and semi-secure environments present their own challenges, since equipment is often exposed to weather and tampering attempts. A Smart padlock addresses this by bringing the same digital credential management to gates, cabinets, containers and other assets that sit outside the main building envelope. This closes a gap that conventional electronic access systems often struggle to cover, since wiring external points is impractical or prohibitively expensive.

## What Organisations Should Consider Before Switching

Moving away from mechanical locks is not purely a technology decision, it also requires thinking through staff training, backup procedures during power or connectivity issues, and how existing doors will be retrofitted. Organisations that plan carefully tend to phase in

digital access gradually, starting with high-traffic or high-risk entry points before expanding further.

Equally important is choosing a system that fits the wider technology landscape. Integration with existing HR platforms, visitor management, alarm systems and CCTV can turn a standalone lock upgrade into a coherent security framework, while open standards reduce the risk of being tied to a single vendor. It is also worth assessing the supplier's support model, update schedule and ability to scale, since needs rarely stay the same as an organisation grows or relocates.

Cost is often the first question raised, but the calculation should include savings from eliminated rekeying, reduced administrative time and fewer security incidents. Over a multi-year period, these savings frequently offset the initial investment in hardware and software.

Vendor lock-in deserves particular scrutiny, since a system that only works with proprietary hardware and software can leave an organisation dependent on one supplier's pricing and roadmap for years after installation. Procurement teams that request interoperability guarantees up front, along with clear data export rights, tend to avoid the costliest surprises later in a system's life. The transition itself rarely needs to happen all at once, and many organisations find that a staged rollout spread gradually across one or two budget cycles produces a noticeably smoother result than a single large capital project.

Data protection deserves equal attention. Digital access systems generate detailed logs about who entered where and when, so organisations need clear policies on retention, who can view this information and how it is used, in line with regulations such as GDPR.4 Running a pilot before full rollout helps surface practical issues early, from unreliable readers to unclear procedures, and gives staff a chance to give feedback, which makes wider adoption considerably smoother.

Security no longer hinges on how many physical keys exist, but on how precisely access can be defined, tracked and adjusted. Organisations that recognise this shift early are better positioned to protect their people, assets and reputation as expectations around accountability continue to rise, particularly as unauthorised key duplication and unrestricted keyways remain a documented, ongoing weakness in facilities still relying on purely mechanical systems.5

- 1Lock-picking made easy
- 2Access control market size, share, latest trends and growth analysis
- 32026 Global Workplace & Occupancy Insights
- 4Principles of the GDPR
- 5Physical security toolbox: lock vulnerabilities and their solutions

## Summary

The organisations managing physical security well in 2026 are not necessarily the ones with the newest hardware, they are the ones that can say precisely who accessed which space and when, and adjust that access in seconds rather than days. Mechanical locks still work as mechanical locks, but they were never built to produce that kind of record, and retrofitting accountability onto a key-based system is far harder than building it into a digital one from the start. The practical path runs through piloting on high-risk entry points first, choosing systems built on open standards rather than a single vendor's proprietary platform, and treating the data these systems generate as a compliance responsibility rather than an afterthought. None of that requires replacing every lock on day one, but it does require treating physical access as seriously as any other system that touches sensitive information and valuable assets.