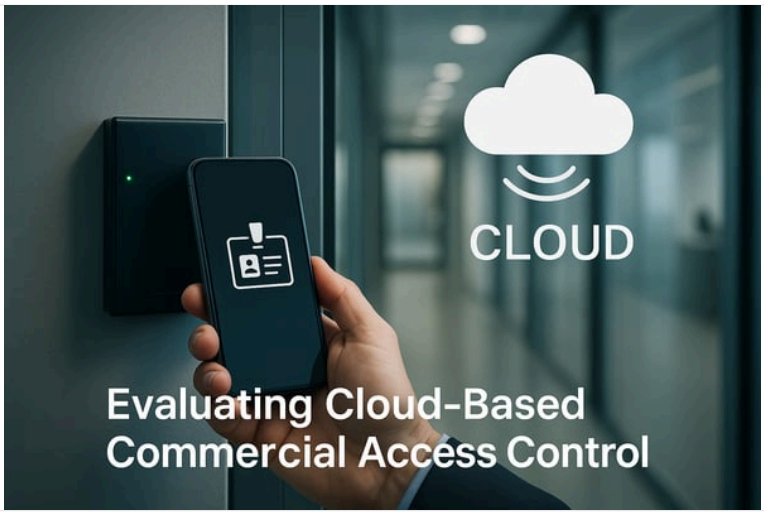
Evaluating Cloud-Based Commercial Access Control Systems

Published September 30, 2025 95 min read



Top 10 Commercial Access Control Solutions (2025)

Executive Summary

A cloud-based access control dashboard enables remote management of doors and users.

Modern commercial access control systems are transforming how organizations secure their facilities. This report ranks the top 10 solutions in 2025, with **Kisi** leading the list as the premier choice. We evaluated each system on key factors like cloud-based management, mobile credentials, integration capabilities, scalability, compliance, and industry-specific features. Kisi distinguishes itself with an intuitive cloud platform, robust mobile access, and open integrations – earning recognition as *"the best business access control system overall"* by an independent review. Other leading contenders include established enterprise systems (Johnson Controls and Honeywell), innovative cloud-native platforms (Brivo, Openpath/Avigilon Alta, Verkada), and specialized providers for wireless locks and multi-site deployments (Salto, Dormakaba, ACRE's Feenics, etc.). Each solution profile in this report details feature sets such as real-time monitoring, visitor management, custom permission controls, third-party integrations (e.g. directory services and workplace tools), security certifications (SOC 2, ISO 27001, GDPR compliance), pricing models, and vertical market focus.

In summary, the top access control systems combine **cloud convenience**, **mobile-first access**, and **enterprise-grade security**. Decision-makers – from security consultants to facility managers – should align their choice with organizational needs: e.g. **Kisi** and **Brivo** for user-friendly cloud management at scale, **Johnson Controls** or **Honeywell** for complex enterprise environments, **Verkada** or **Openpath (Avigilon Alta)** for unified security with video integration, and **Salto** or **Dormakaba** for advanced lock hardware solutions. The following sections present our ranking methodology, the full top-10 list, detailed solution profiles, a feature matrix, and tailored recommendations by use case.

Methodology for Ranking

Our ranking is based on a comprehensive analysis of each solution's capabilities, security credentials, market reputation, and applicability across industries. We gathered data from official product documentation, security certifications, customer case studies, and trusted industry reviews (including analyst reports and security technology blogs). Key evaluation criteria included:

- **Core Feature Set:** Availability of cloud-based management dashboards, mobile credential support, real-time activity logs and alerts, visitor management modules, and advanced permission controls. For example, mobile/cloud access is now considered a *"must-have"* for modern systems, so solutions lacking robust mobile apps or remote management scored lower.
- **Integration & Ecosystem:** Ability to integrate with third-party services such as identity providers (Google Workspace, Microsoft Azure AD/Entra ID, Okta), communication tools, video surveillance systems, and building management platforms. Open API availability and support for standard hardware (Mercury controllers, open protocol readers) were positives. Systems with proprietary lock-in hardware or siloed software were noted.

- **Scalability & Reliability:** Performance in multi-site or enterprise deployments, offline reliability (continued operation during network outages), and high user/door counts. We considered any limits on expansion (e.g. reader or event caps) and whether the architecture is truly cloud-scalable or an on-premises system retrofitted with cloud connectors.
- **Security & Compliance:** Certifications such as SOC 2 Type II and ISO 27001, compliance with GDPR and other data protection laws, and adherence to industry security standards (encryption, NDAA-compliant hardware, FIPS, etc.). Verified certifications (SOC 2, ISO 27001) were weighted heavily to ensure vendor trustworthiness.
- **Pricing Transparency & TCO:** Clarity of pricing models (published pricing vs. custom quotes), licensing fees for features like mobile credentials, and overall cost-effectiveness. Solutions with clear, published pricing (e.g. Kisi) scored points for transparency, whereas legacy providers requiring custom quotes were assessed qualitatively.
- **Industry Adoption & Customization:** Evidence of success in specific verticals (e.g. coworking spaces, enterprise offices, healthcare, education, multifamily residential). We looked for features tailored to industry needs – for instance, integrations with property management systems in multifamily, or compliance with healthcare and government security regulations for enterprise. Each solution's "best for" categories were considered (e.g. Kisi is noted for SMB and offices, Honeywell for large facilities like airports).

Each system was researched with up-to-date information as of mid-2025. Our methodology ensured an unbiased, feature-by-feature comparison to provide professionals with a clear understanding of the landscape.

Full Ranking Table of Top 10 Solutions

Below is an overview of the top 10 commercial access control solutions for 2025, ranked in order. This table lists each solution, its general solution type, and a key strength or ideal use-case:

RANK	SOLUTION	SOLUTION TYPE & IDEAL USE-CASE
1.	**Kisi**	Cloud-based, mobile-first access platform – best overall for modern offices and SMB, with broad integrations.
2.	**Johnson Controls (C•CURE)**	Enterprise on-prem & cloud-hybrid solution – ideal for large enterprises and high-security facilities requiring extensive integration (video, fire, intrusion).
3.	**ADT**	Full-service security solution – customizable for all sizes, with 24/7 monitoring and integration of access, video, and alarms (popular for retail, franchises, etc.).
4.	**ACRE (Feenics/Vanderbilt)**	Cloud-enabled Mercury-based systems – flexible for enterprises that prefer non-proprietary hardware and need features like emergency lockdown and visitor kiosks.
5.	**Verkada**	Hybrid-cloud security platform – ideal for IT-centric organizations seeking unified access + video on a simple cloud interface, scalable from ten to thousands of doors.
6.	**Brivo**	Pioneering cloud access control – great for multi-site businesses and multifamily, offering robust API integrations and user-friendly management via web/mobile.
7.	**Avigilon Alta (Openpath)**	Mobile-centric cloud access (Motorola Solutions) – suited for modern workplaces and multifamily communities, with touchless smartphone entry and strong video intercom integration.
8.	**Dormakaba**	Integrated hardware-software solution – global leader in locks and entrance systems, best for enterprises needing seamless electronic locks (doors, turnstiles, etc.) and hotel/hospitality integrations.
9.	**Salto**	Wireless smart lock platform – ideal for campus environments (education, hospitality) needing flexible keyless entry solutions and easy scalability with cloud management.
10.	**Honeywell**	Enterprise security suite – proven for large campuses and critical infrastructure (airports, hospitals) with comprehensive access control tied into fire, HVAC, and building automation.

Table Note: Avigilon Alta is the rebranded Openpath cloud access product under Motorola Solutions. ACRE's portfolio includes Feenics (Keep) for cloud access and Vanderbilt Industries for on-prem systems. Johnson Controls includes Tyco Software House (C•CURE 9000) and Kantech lines. Each solution's detailed profile is provided in the next section.

Detailed Profiles for Each Solution (1–10)

1. Kisi

Overview: Kisi is a cloud-based access control provider known for its easy-to-use software and seamless mobile access. As a true cloud solution, Kisi enables administrators to manage doors and credentials from anywhere via a web dashboard or mobile app. It blends **smart hardware** (proprietary Kisi Controllers and Reader Pros) with an open platform that integrates into existing IT and security systems. Tech-savvy businesses appreciate Kisi's user-friendly interface and the elimination of on-premises servers.

Key Features:

- **Cloud Management:** Centralized cloud dashboard for real-time monitoring, remote unlocks, and audit logs. Administrators can instantly adjust permissions or view door events from any location. The system is continuously updated with new features via the cloud.
- **Mobile & Keyless Access:** Robust mobile app (iOS/Android) that turns smartphones into keys, supporting Bluetooth, NFC, and even *Apple Wallet* badges for entry. This provides a frictionless, touchless entry experience. Traditional keycards/fobs (128-bit AES encrypted) are also supported for hybrid use.
- **Integration & API:** Open API and dozens of out-of-the-box integrations. Kisi can sync with **directory services** (Azure AD, Okta, Google Workspace) to automate onboarding/offboarding, with **communication tools** like Slack for entry notifications, and with **visitor management** platforms (e.g. Envoy) to streamline guest access. It also integrates with IoT devices (wireless locks from Allegion, security cameras, alarm panels) to create a unified system.
- **Scalability:** Suitable for a single door up to enterprise multi-office deployments. Kisi's cloud architecture and *One Security Platform* approach scales globally while maintaining centralized control (Source: getkisi.com). (Note: Very large deployments may require multiple controllers – each Kisi Controller supports 4 doors – which is a consideration for sites with hundreds of doors.)
- **Visitor Management:** Offers a built-in **visitor access** module that issues temporary QR code passes or link-based credentials to guests for app-free entry. This modernizes visitor check-in and works seamlessly with Kisi-controlled doors.
- **Real-time Monitoring:** Provides live door events, customizable alerts (e.g. door left open, forced entry) and reporting analytics. Administrators can receive instant notifications for critical events and review audit trails per user or door.
- **Custom Permissions:** Granular access rules by user groups, schedules, and roles. Kisi supports time-based access (e.g. only during business hours or specific shifts) and location-based restrictions across multiple sites. Global offices can be managed under one system with local segmentation of permissions.
- **Remote Unlock & Admin:** Doors can be remotely unlocked or locked down via the Kisi app or web, supporting use cases like letting in delivery personnel off-hours or initiating an emergency lockdown across a facility.
- **Security & Compliance:** Kisi is independently certified for **ISO 27001** and **SOC 2 Type II**, underscoring strong data security practices. It complies with GDPR, CCPA, and NDAA requirements. Data is encrypted in transit and at rest, and regular penetration tests are conducted to ensure system resilience.
- **Pricing:** Kisi is one of the few in this sector with transparent pricing. The hardware (controllers and readers) is sold upfront (roughly $599–699 per reader and $899 per controller) and cloud software is subscription-based around ~$49 per door per month. There are no per-user fees, and mobile credentials are unlimited with the service – offering a cost-effective model relative to legacy systems that charge per credential.
- **Industry Use Cases:** Small and medium businesses are a sweet spot for Kisi, including coworking spaces, modern offices, fitness studios, and educational institutions. Enterprises with a "cloud-first" IT strategy also adopt Kisi for its flexibility. Its ability to integrate with industry-specific software (e.g. Optix for coworking, Club management systems for gyms) makes it adaptable. Enterprise clients use Kisi to manage global offices with unified policies.

Notable Strengths: Kisi's ease of installation and setup is frequently praised – it can retrofit on any electric strike or magnetic lock with minimal wiring, often in minutes. Its mobile-centric approach and *unified app* (employees, admins, and even guests all use one app or link-based system) stand out, especially compared to some competitors that require multiple apps for different functions. Integrations (20+ and growing) allow Kisi to fit into any tech stack, automating workflows like revoking access when an HR system marks an employee as terminated. Also, **Kisi's commitment to security** (SOC 2, ISO 27001) is on par with industry leaders, reassuring for IT and security teams.

Potential Drawbacks: As a proprietary system, Kisi does require using its controllers and readers (though they work with standard door hardware). This "closed hardware" approach means existing third-party panels generally need replacement when switching to Kisi. However, Kisi's open API mitigates vendor lock-in on the software side by integrating with other systems. For very large facilities (hundreds of doors), installing many Kisi controllers could be a logistical consideration, though the cloud software scales without issue. Finally, while Kisi now offers visitor management, it is relatively basic (primarily QR code/email links) and not as feature-rich as some dedicated visitor systems – organizations with heavy visitor workflows might integrate a partner solution for additional capabilities.

2. Johnson Controls (Tyco Software House C•CURE & Kantech)

Overview: Johnson Controls (JCI) offers some of the most established access control systems on the market, chiefly the **Software House C•CURE 9000** platform and **Kantech** systems (as a result of JCI's merger with Tyco). These solutions have been industry staples for decades in large enterprise, government, and high-security environments. JCI's portfolio is evolving to include cloud-managed options like *C•CURE 9000 Cloud* and *Tyco Cloud*, but their core offerings remain robust on-premises systems with optional cloud hosting. JCI systems are known for **scalability** (handling thousands of doors and cardholders), deep integration with building security systems, and compliance with stringent government standards.

Key Features:

- **Cloud or On-Prem Deployments:** Traditionally deployed as on-site servers with thick-client software for control, C•CURE 9000 can now be cloud-hosted or run in a hybrid model. Johnson Controls introduced **C•CURE Cloud** (hosted on AWS) which maintains full feature parity while reducing on-prem IT footprint. This cloud service is built on a SOC 2-compliant infrastructure and even supports government FICAM standards for federal deployments. For smaller installations, JCI's **Kantech** line (e.g. EntraPass software) offers simpler web-based management or hosted options.
- **Enterprise Scalability:** Capable of managing *tens of thousands of users and events per day* across multiple facilities. The architecture supports distributed processing – e.g., **C•CURE 9000** can use clustered application servers and the **iSTAR controllers** handle local decisions if network is lost. JCI claims essentially unlimited door capacity in their enterprise edition, making it suitable for very large campuses and global corporations.
- **Hardware Integration:** JCI's systems use **open hardware** in many cases – for instance, Kantech controllers and newer iSTAR Edge devices are Mercury-compatible or open standard, allowing some flexibility. However, C•CURE traditionally uses proprietary iSTAR panels. JCI solutions integrate tightly with **HID readers** (including biometric readers) and support multi-tech credentials (Prox, iCLASS, DESFire, etc.). The hardware portfolio is broad: from IP door controllers to encrypted smart card readers and wireless lock integrations.
- **Software & Analytics:** The C•CURE software suite is feature-rich: real-time alarm monitoring, threat level management (e.g., lockdown modes at the press of a button), muster reporting for emergencies, and a rules engine to program complex security workflows. It includes an identity management module and can integrate with HR databases for provisioning. The UI is complex but highly customizable – security operators can display interactive floor plans with door status, and set up workflow-based responses to incidents. JCI also offers **reporting and analytics** for compliance (e.g., PIAM – physical identity and access management features).
- **Visitor Management:** A *native visitor management* module is available (e.g., *C•CURE 9000 Visitor Management*), allowing pre-registration of guests, badge printing, host notifications, etc. This is beneficial for enterprises that want a one-stop solution. However, it may not be as modern as specialized visitor apps; many JCI customers also integrate third-party visitor systems.
- **Mobile & Remote Access:** Historically a weakness – older JCI systems were built for PC-based control. However, JCI released the **Honeywell/Johnson Controls Secure App** (for its security products line) which provides mobile monitoring and basic door control (Source: play.google.com). In practice, many JCI deployments use *HID Mobile Access* for mobile credentials (since HID Global hardware is often used) – meaning employees can tap their phone via BLE/NFC to HID readers to enter. *Apple Wallet support* for employee badges is not natively mentioned, but using HID's platform it can be achieved. Full mobile administration (adding users, remote unlocks via app) is still catching up but is improving via the new web interfaces and apps.
- **3rd-Party Integrations:** Johnson Controls solutions excel in integrations for **video surveillance, alarms, and building systems**. C•CURE, for example, integrates with **video management systems** (like American Dynamics victor, ExacqVision, Milestone) to link door events with video. It also integrates with **intrusion detection** panels and intercom systems for unified alarm management. For IT integration, JCI supports Active Directory sync for user data, and OSDP secure channel for reader communications. There are SDKs and APIs for custom integrations as well. Some cloud integrations (like SCIM provisioning or Azure AD user sync) may not be as plug-and-play as in newer cloud-native solutions, but can be achieved with professional services.
- **Compliance & Security:** JCI's access control is trusted in high-security environments – it offers end-to-end encryption (AES 256) between controllers and software, and options for **FIPS 140-2** validated components for government use. The cloud-hosted offerings are built on secure platforms (OpenShift on AWS) with SOC 2 compliance. JCI also complies with industry specific standards (for example, their PIV support for government credentials via FIPS 201). The company emphasizes cybersecurity practices and has a dedicated product security team; their systems undergo regular threat modeling and updates (the **Johnson Controls Security Lifecycle** program).
- **Pricing:** Johnson Controls solutions are sold through integrator partners and pricing is **quote-based**. Typically there are license fees per door or per reader for the software, plus annual software maintenance contracts. Enterprise systems like C•CURE have a higher upfront cost and ongoing support fees. The newer cloud subscription model (Tyco Cloud) likely shifts to recurring SaaS fees. *Pricing transparency is low* – customers must engage a certified dealer for quotes. As a frame of reference, total cost per door (including hardware, software license, and installation) can be on the higher end (often $1500–$3000/door in enterprise scenarios), but it comes with robust functionality.

Notable Strengths: Johnson Controls (via Tyco's brands) has a **proven track record** in large-scale deployments – many Fortune 500 companies, government agencies, and critical infrastructure sites rely on C•CURE or Kantech. The systems are extremely **feature-rich and customizable**, supporting complex security policies (e.g., dual authentication at certain doors, anti-passback rules, lockdown scenarios, etc.). Integration breadth is a major strength:

one can manage video, access, and alarms in one interface for holistic security management. The ability to mix and match hosted vs on-prem components provides flexibility; for example, a customer could have an on-prem server at HQ and use a cloud portal for regional sites. Also, **scalability and reliability** are top-notch – these systems rarely have hard limits that a normal enterprise would hit, and they support redundancy and failover for high availability.

Potential Drawbacks: The trade-off for power and scale is complexity. JCI's interfaces (C•CURE in particular) can be **less user-friendly** and require certified technicians for setup and changes. Day-to-day management might demand more training compared to the simplicity of newer cloud entrants. For smaller organizations without dedicated security IT staff, the JCI systems can be overkill. Additionally, **cost is significant** – not just initial cost, but ongoing maintenance and the need for professional support. The reliance on proprietary elements (in some cases) can create vendor lock-in, though JCI has moved toward openness with Mercury hardware. Another drawback has been slow adoption of some modern conveniences – e.g., *no native Apple/Google Wallet integration* out of the box (unlike Kisi or Brivo), and until recently no unified mobile app for administrators. However, JCI is addressing some of these with its evolving cloud portal and mobile offerings. Lastly, because JCI systems are typically installed by third-party integrators, the **customer experience** can vary – responsiveness of support depends on the local dealer, which can be a pain point versus direct support models from some cloud providers.

3. ADT Access Control

Overview: ADT is a well-known name in security, and its commercial division provides integrated access control as part of broader security offerings. Rather than a single proprietary platform, **ADT acts as a solutions provider/integrator**, often delivering a customized system using hardware/software from various manufacturers (including their own branded solutions and partners). ADT's value proposition is a **one-stop shop**: they design, install, monitor, and service the entire security system – including access control, intrusion alarms, and video surveillance – especially for small and mid-sized businesses. ADT's long history (since 1874) in alarm monitoring gives it a strong service backbone for 24/7 support.

Key Features:

- **Customizable Solutions:** ADT doesn't force a one-size platform – they tailor the system to client needs. For example, a solution might use **Honeywell or Lenel controllers** in a larger install, or **Brivo/Alarm.com Cloud** for smaller ones. ADT's own branded access control platform (formerly ADT Select or ADT Enterprise) often leverages Mercury-based panels with ADT's software wrapper. This flexibility means an ADT system can be as simple or advanced as needed, from a single-door key card system up to a multi-site enterprise deployment. The configuration is *completely customizable* to fit requirements and budget.
- **Integrated Security Features:** A hallmark of ADT's offering is integration of **access control with video surveillance and intrusion detection**. For instance, an ADT access system can link doors to ADT cameras so that when a door is opened, recording is triggered. Likewise, it can tie into alarm systems – e.g., using a door forced-open event to trigger an alarm or notifying the intrusion panel status on the same app. Many competitors offer integrations, but ADT's advantage is they deliver it as a unified package (and often with a single interface for the end-user, such as ADT's Pulse or Control apps for SMB).
- **Remote Management:** ADT provides **remote monitoring and management** tools so customers can control their system off-site. ADT's business mobile app (often ADT Control for Business) allows owners to lock/unlock doors, receive alerts, and even manage user codes or cards remotely. Small businesses, for example, can arm/disarm alarms and unlock doors from a phone. ADT emphasizes that the *entire system can be controlled remotely*, reflecting the push toward cloud connectivity.
- **Access Methods:** Typical ADT installations support **key cards, fobs, PIN codes, and mobile credentials**. ADT advertises the ability to use mobile phones as access credentials (likely using either HID Mobile or Alarm.com's mobile credentials platform). Biometric readers or intercoms can also be incorporated if needed. They also offer **two-way intercom stations** at entry points, allowing security or staff to communicate with visitors before granting access – useful for gated entries or lobby doors.
- **Visitor & Contractor Management:** While ADT doesn't have a proprietary visitor management app, they often configure systems to accommodate visitor entry via intercom or keypad. They can integrate systems like **Envoy or Traction Guest** upon request. For contractors or deliveries, ADT's solutions often include scheduled access codes or remote unlock via the business owner's app. The focus is on making it convenient for business owners to authorize visitors without having to be on-site.
- **Monitoring Services:** A unique aspect is ADT's **24/7 professional monitoring** option. For example, if the access system is tied to an alarm and a forced entry occurs after hours, ADT's monitoring center will respond and dispatch authorities if needed. This service layer sets ADT apart from purely DIY or unmonitored systems. It essentially outsources part of the security management to ADT's team for an additional fee, which many businesses find valuable.
- **Scalability:** ADT serves all scales, but is especially popular in **small to mid-size businesses and retail chains**. They highlight that the system can *scale up or down as business needs change*. For instance, adding new doors or locations can be done under the ADT umbrella easily. That said, very large enterprises with complex needs might opt for specialized systems (which ADT could still implement as the installer). ADT Commercial (a separate division) handles bigger projects using enterprise-grade platforms (they might deploy LenelS2 or S2 NetBox for a corporate campus under their management).

- **Security & Compliance:** ADT leverages the security of whichever underlying system they install. They ensure signals and data are encrypted (especially alarm signals to their monitoring centers). ADT itself is UL certified for alarm installations and likely ensures any cloud components are on secure infrastructure. However, ADT does not publicly tout SOC 2 or ISO 27001 in the way pure software providers do, since they are more of an integrator. For compliance (like GDPR or privacy), they defer to the platforms used (many ADT-provided cloud systems are based on Alarm.com which has robust cloud security).
- **Pricing:** ADT's model typically involves upfront installation costs plus a recurring subscription for monitoring and cloud access. **Pricing is not transparent** publicly; it's provided via free quote consultations. However, ADT often runs promotions. For a small business, one might pay a few hundred dollars for equipment/installation per door and then a monthly fee (which could be on the order of $40-$100/month for a bundle of alarm + access + video monitoring). The quote is customized to include all needed components. ADT's strength is offering *financing or leasing* of equipment in exchange for multi-year service contracts, making it a predictable operational expense for businesses.

Notable Strengths: The key strength of ADT is **simplicity and support**. Business owners who do not have dedicated security or IT staff can rely on ADT to handle the design, installation, and ongoing management of the system. ADT's solutions are **professionally installed** and include training, which removes a lot of hassle. The integration of intrusion alarm monitoring with access control is also a big plus – one vendor covers both, so there's no finger-pointing between separate alarm and access companies. ADT's long-standing central monitoring service is a differentiator; few others on this list offer live monitoring of access events. For multi-location retail or franchises, ADT can provide a consistent solution across all sites and a single point of contact for support. Additionally, ADT's systems are quite **feature-complete for SMB needs**: remote management, basic analytics (like access reports, time-and-attendance data), and the peace of mind of a reliable brand.

Potential Drawbacks: As ADT uses various underlying technologies, the **feature set can vary**. You're somewhat reliant on ADT's choice of platform, which might not be as cutting-edge as some specialized competitors. For example, ADT might not immediately offer features like Apple Wallet employee badges or advanced visitor QR codes unless their chosen platform supports it. There is also typically **less transparency** in the technology – the user is interfacing mainly with ADT's portal or app, which could mask a third-party system. If a customer wanted to self-manage at a deep level (e.g., integrate new software via API), it could be difficult with ADT unless they facilitate it. Another drawback can be **cost over time** – ADT's convenience and service come at a premium. Long-term contracts with automatic renewals are common, and canceling early can incur fees. Some customers report that proprietary elements or contract terms make switching away from ADT costly. Finally, ADT's focus on service means the **user experience might be less configurable** by the customer – for instance, advanced custom rules or integrations would require engaging ADT support rather than DIY. For highly tech-oriented clients who prefer direct control and customization, this can be limiting. Overall, ADT is ideal for those who want security handled for them, but less so for those who want to tinker or have unique, evolving tech integration needs.

4. ACRE (Feenics Keep, Vanderbilt, Open Options)

Overview: ACRE is a parent company that has aggregated several access control brands, including **Feenics (Keep)**, **Vanderbilt Industries (ACT)**, **RS2 Technologies**, and **Open Options**. Through these brands, ACRE offers a comprehensive portfolio from pure cloud access control to on-premises enterprise systems. In our context, we focus on ACRE's flagship cloud platform, *Feenics Keep*, and related offerings. ACRE's solutions are known for leveraging **non-proprietary Mercury hardware** extensively, giving customers flexibility to avoid vendor lock-in. They are feature-rich and standards-based, appealing to enterprises and integrators who value openness.

Key Features:

- **Cloud-Based Platform (Feenics):** Feenics (acquired by ACRE in 2021) offers *Keep by Feenics*, a true cloud access control solution hosted on Amazon Web Services. Keep is built as a multi-tenant SaaS platform, meaning integrators or end customers can manage access control via a web browser without local servers. It supports all core functions (add users, assign credentials, set schedules, monitor events) through an intuitive interface. A notable feature is a built-in **"Emergency Lockdown"** capability that can secure all doors instantly via the cloud in crisis situations. Also, Feenics supports **mass notifications**, so security admins can send out alerts to employees during emergencies.
- **Open Hardware (Mercury Powered):** ACRE's systems (Feenics, RS2, Open Options, and even Vanderbilt's enterprise systems) are largely built on **Mercury Security** controllers. Mercury is an industry-standard hardware platform used by many vendors, which means ACRE solutions can often work with existing Mercury boards or at least be migrated to/from other Mercury-based systems with minimal hardware swap. This non-proprietary approach gives customers freedom to change software down the line without ripping out all controllers. It also ensures compatibility with a wide range of reader hardware (HID, Allegion Schlage, NXP, etc.).
- **Integration Capabilities:** Feenics Keep offers an **open RESTful API** and a growing list of integrations (approximately 20+ pre-built integrations as of 2024). These include linking with **HR systems** like Workday for automatic provisioning of access when a new employee is added, and with **visitor management kiosks** (Feenics has a native visitor management module and a tablet-based kiosk app). It can integrate with identity management (via Okta or Azure AD using SCIM), and with third-party video platforms – although Genea's analysis noted that Feenics had *fewer video management integrations* out-of-the-box compared to some competitors. Notably missing were direct integrations with Cisco Meraki Video, Rhombus, or Eagle Eye at the time of that analysis. However, basic alarm outputs can trigger external systems and vice versa. Elevator control integration is supported but perhaps not as extensive as leaders (fewer options for destination dispatch, etc., were mentioned).

- **Mobile & Credentials:** Feenics supports traditional cards/fobs and has implemented OSDP for secure reader communications. For mobile access, Feenics itself did not have a proprietary mobile credential as of 2024 (no Apple/Google Wallet integration natively and limited mobile app functionality for end-users). However, since it's Mercury-based, it can leverage HID Mobile IDs if HID readers are used, or other BLE/NFC reader credentials. The emphasis of their mobile app was more on admin control rather than end-user door unlocks. This is a comparative weakness in user experience where more mobile-centric rivals shine.
- **Dashboard & User Experience:** The Feenics web dashboard is modern but was cited to have **fewer features** compared to top competitors. It covers the essentials: live events, reporting, user management, and configuration, but might lack some advanced analytics or polished UI components that others boast. Feenics does allow custom reporting and has a rules engine for basic automation. One advantage is the ability for multi-tenant management – an integrator can manage multiple customer sites from one interface, which is great for managed service providers. From the end-customer perspective, it's straightforward for security personnel to use for day-to-day tasks.
- **Visitor Management:** ACRE's Feenics includes a **native visitor management** system. They offer a Visitor Management (VM) Kiosk application that can run on a tablet for self sign-in. This ties into the Keep platform so that when a visitor is registered, a temporary credential can be issued and tracked. This is a nice built-in feature, although, as noted, the visitor module is relatively basic by enterprise standards (check-in, badge print, notify host).
- **Scalability:** ACRE's solutions can scale to enterprise levels. Keep (Feenics) being cloud-based inherently can scale horizontally as AWS allocates resources. The underlying Mercury hardware can handle large numbers of readers and transactions (each Mercury panel can support dozens of readers and those panels can be networked). For example, a single Feenics instance could manage multiple sites with hundreds of doors each. ACRE also still sells on-prem systems (like Vanderbilt SMS or RS2 AccessIT) for those who prefer localized control; those are also scalable but with the typical constraints of server infrastructure.
- **Security & Compliance:** ACRE as a company doesn't heavily publicize certifications like SOC 2 on their marketing, but given Feenics is hosted on AWS, it inherits a lot of AWS's security compliance (ISO 27001, SOC 1/2 for the infrastructure). The platform uses TLS encryption for all communications and can enforce 2FA for admin login. One can infer that they likely do regular security audits. However, lack of explicit SOC 2 certification mention in literature might be a concern for some customers (it was listed as a drawback by at least one analyst, possibly implying it hadn't achieved certain compliance attestations yet). On the hardware side, Mercury controllers are UL-listed and OSDP secure channel capable, aligning with industry best practices.
- **Pricing:** ACRE's pricing structure for Feenics Keep is typically subscription-based per door per year. Genea's report explicitly noted "Pricing" as a drawback without elaboration, suggesting it might be relatively high or at least not transparent. Enterprise software from Vanderbilt/RS2 often has license fees. Feenics likely sells through integrators who set the end pricing. So while open hardware could reduce costs on reusing gear, the software and support might still be significant. There may also be additional fees for certain integrations or mobile apps (and indeed, Genea noted that some competitors charge extra for mobile credentials; Feenics possibly requiring HID subscriptions for mobile IDs might fall under that concern).

Notable Strengths: ACRE's top strength is **flexibility and openness**. By using Mercury hardware across many of its products, ACRE empowers customers to avoid vendor lock and mix components. If you invest in an ACRE system and later decide to switch software, your controllers and readers could be repurposed under another Mercury-compatible system (e.g., Genetec or Lenel). This is a stark contrast to proprietary systems where a platform change means replacing all hardware. For organizations and integrators, that risk mitigation is valuable. Additionally, ACRE covers *both* ends of the spectrum – from **cloud-first (Feenics)** to **on-premises (Vanderbilt/RS2)** – so customers can find a solution within the family that fits their IT philosophy. Feature-wise, ACRE systems include all enterprise capabilities one would expect: zone-based anti-passback, elevator control, detailed access rule configurations, etc. The **native visitor management** and **Mercury-based lockdown features** are pluses for safety-conscious clients. Because ACRE products are often integrator-delivered, they come with **robust support channels**, and the platform is integrator-friendly (e.g., multi-tenant capabilities for managed services).

Potential Drawbacks: Compared to some competitors, ACRE's user interfaces and polish might lag a bit. The critique that the dashboard has *"limited features compared to others"* indicates that user experience could be improved – perhaps reporting is not as slick, or certain modern conveniences (like drag-and-drop scheduling or easy bulk edits) aren't as smooth. Also, while Feenics is cloud-based, it was noted as being *"not as streamlined as other non-proprietary, cloud competitors"*, hinting that newcomers like Kisi or Brivo may currently offer a more intuitive experience. Another drawback is the **mobile credential gap** – ACRE doesn't have its own mobile access app for end-users (as of mid-2025, to our knowledge). This means customers must rely on third-party mobile solutions (e.g., HID Mobile) which can add cost and complexity (and indeed, one competitor analysis called out no Apple/Google wallet and limited mobile functionality as Feenics gaps). Moreover, **some features require additional fees or products** – e.g., visitor kiosk hardware/license, or if one wants video integration, they might need a Vanderbilt video system or separate VMS, since it doesn't bundle video in the base offering. Pricing being somewhat opaque and likely on the higher side for cloud (due to enterprise focus) can be a deterrent for budget-sensitive buyers. Finally, ACRE's multi-brand lineup can itself be confusing – prospective customers might not know whether to implement Feenics vs. Vanderbilt ACT, etc. without consulting an ACRE integrator, whereas a single-brand company has a clearer pitch. In summary, ACRE's solutions are powerful and open, but not always the most modern in interface or mobile experience, making them a better fit for those prioritizing integration and scalability over sleek design.

5. Verkada

Overview: Verkada is a newer entrant (founded in 2016) that has quickly made a name in the physical security space with its **cloud-managed**, all-in-one approach. Initially known for cloud-connected security cameras, Verkada expanded into access control and environmental sensors, branding itself as a unified building security platform. Verkada's access control offering, often referred to as **Verkada Command for Access**, emphasizes plug-and-play hardware,

centralized cloud management, and tight integration with video surveillance. It's targeted at organizations that want modern, IT-friendly systems with minimal infrastructure – Verkada famously touts having *"no on-prem servers"* required. The solution is subscription-based, combining hardware (smart door controllers) with a software license that covers continuous updates and cloud service.

Key Features:

- **Hybrid-Cloud Architecture:** Verkada uses a **"hybrid cloud"** model – door controllers (like the Verkada AC41 4-door controller or the AD32 door reader interface) handle real-time decisions at the edge, but all management and configurations are done through Verkada's cloud platform (Command). There are *zero on-site servers*; simply connect controllers to the internet and they are online in minutes. If the network goes down, controllers continue to enforce access based on last known config (thanks to local storage/processing) and will sync events once connectivity returns (Source: verkada.com). This ensures high availability and offline resilience.

- **Cloud Management (Command):** The Verkada Command cloud interface is unified across all Verkada devices (cameras, doors, sensors). For access control, Command provides a **web and mobile app** for administrators to manage users, schedules, and view events. It features an extremely user-friendly design, consistent with modern SaaS applications. From any browser, an admin can drag-and-drop to assign doors to access groups, set unlock schedules, or review an access event with associated video footage side-by-side. Command includes **visual floor plans**, centralized user directories, and custom alert rules (e.g., alert if a door is forced). The mobile app allows for door unlocks on the go and receiving push notifications.

- **Video Integration & Context:** Verkada's standout proposition is **native integration of access control with video**. If you have Verkada cameras watching an entrance, the Command platform will tie access events (door unlocks, door open/close, rejected entry) with the corresponding video clip automatically. This means a security officer can click on an access event and immediately see who walked through the door, greatly enhancing situational awareness. The system also supports analytics like **tailgating detection** – using camera analytics to see if two people enter on one credential swipe and flagging that as a tailgating alert. Verkada also recently added an **intercom door station** product, fully integrated, so video intercom calls and door unlocks via intercom tie into the same system.

- **Mobile Credentials & Touchless Entry:** Verkada supports **Bluetooth Low Energy (BLE)** based mobile credentials through its Verkada Pass app. Users can unlock doors using their phone via the app or even set up **touchless entry**: as a person approaches, the Bluetooth reader can detect their phone and unlock without needing to take it out (this is configurable). They do not yet support Apple Wallet or NFC tap from phone – it's done via the Verkada app and Bluetooth in the background. Additionally, Verkada offers standard badge/fob support, and interestingly, also can use **license plates as credentials** in some scenarios (tying with their LPR cameras). The system is flexible: any combination of cards, fobs, Verkada's smartphone app, or even **"remote unlock links"** (send someone a link to remotely open a door) can be used.

- **Ease of Installation & Migration:** Verkada's hardware is designed for simplicity. Controllers are PoE-powered and come with detachable screw terminals for wiring doors, making installation straightforward for electricians. For retrofits, Verkada highlights that their AC41 controller can **work with existing door hardware and readers** – meaning an organization can keep their door strikes/magnets and even Wiegand readers if desired, swapping out only the control panel. This reduces upgrade friction. Verkada also has a feature to import existing cardholders and credentials via CSV or integrate via SCIM (e.g., from Azure AD) to onboard users quickly. Essentially, Verkada tries to make switching from a legacy system as easy as possible, leveraging compatibility where feasible (e.g., Wiegand reader inputs).

- **Integrations & APIs:** Verkada provides a set of **open APIs, webhooks, and SDKs** for customers to integrate its system with other software. There's an official Verkada API for pulling events or triggering actions, and they support **SCIM** (System for Cross-domain Identity Management) and **SAML SSO** for user directory integration. For example, one can integrate Verkada with Okta or Azure AD to automatically manage users and access groups. Verkada's **Marketplace** showcases integrations such as with identity management (e.g. syncing with HR databases) and Slack or Teams for notifications. They also have webhooks that can notify external systems of events. Compared to some older systems, Verkada's integration approach is much more modern and IT-friendly.

- **Security & Compliance:** Verkada has invested heavily in cloud security. The platform and products have achieved **SOC 2 Type II** and multiple **ISO 27001/27017/27018** certifications (covering information security and cloud privacy). Verkada encrypts data in transit and at rest, and uniquely, because video footage and some data are stored on device and in cloud, they implement end-to-end security. They also introduced an **Enterprise Encryption Key** option where customers can hold their own keys for video footage (so Verkada cannot view it – addressing privacy concerns). From a privacy perspective, Verkada supports GDPR compliance and has features like data retention policies and access logs for who viewed video or accessed data. Their hardware is NDAA compliant (no banned components) and FIPS 140-2 certified encryption modules are used, catering to government requirements. They also undergo annual penetration testing and continuous security monitoring.

- **Scalability & Updates:** Verkada's system is built to scale – whether you have **10 doors or 10,000 doors, across global sites**. Because all sites feed into the same cloud dashboard, it's inherently multi-site friendly. There's no practical upper limit stated on readers or users; Verkada regularly references customers with dozens of locations managed centrally. The cloud nature also means **automatic firmware and feature updates** – new features roll out monthly to the platform with no downtime, and devices get updates over the internet. This keeps the system improving over time without costly upgrade projects.

Notable Strengths: Verkada's primary strength is the **unified, cloud-native experience**. It brings the ease of consumer tech to enterprise security. IT administrators love that there are no DVRs, NVRs, or on-prem servers to maintain – just connect hardware and manage everything centrally. The **tight integration of video and access** is a big selling point; it provides context to access events effortlessly and can significantly speed up investigations (e.g., see who piggybacked through a door without manually cross-referencing video). Verkada's user interface is often praised for its simplicity and modern feel – minimal training is needed for staff to use it. Another strength is **fast deployment**: adding a new door or camera can be done in minutes and appear in the cloud ready to configure. Verkada is also expanding into new areas (environmental sensors, alarms, visitor management with Verkada Guest), all feeding into one platform, which is attractive for customers wanting to consolidate vendors. From a business standpoint, Verkada's **all-inclusive licensing** (hardware + software warranty + support in one price) makes costs predictable and support straightforward. Finally, being a Silicon Valley tech-driven company, Verkada is quick to add features that customers demand (for instance, they introduced **Face ID unlock for the mobile app** and **mask detection** analytics during COVID times, showcasing agility). It's regarded as a **"simple, scalable security system"** by customers ranging from schools to corporate offices.

Potential Drawbacks: Verkada's approach has a few caveats. Firstly, it is a **proprietary ecosystem** – you largely have to use Verkada's controllers and software together. While they allow using existing door hardware and readers, the brains are Verkada's, and if you ever left Verkada, you'd likely need to replace those controllers. This is common with many systems, but contrasts with Mercury-based open systems. Also, Verkada's readers currently don't support some high-security card formats except through third-party readers (their controller can accept Wiegand, but their own reader is 13.56MHz only). Another drawback discussed in some security circles was **privacy** – early on, Verkada had an internal misuse incident (employees viewing camera feeds improperly), which the company addressed with stricter controls. While they have since doubled down on privacy and encryption, some organizations might be wary of placing critical security on a cloud platform managed by a third party. Additionally, **Verkada's cost** can be high: you pay upfront for hardware and an annual license (typically sold in 5-10 year blocks). Over a long period, it might cost more than self-managed solutions, though you get continuous updates for that price. There's also **less customization** available compared to traditional systems – you more or less operate within Verkada's provided feature set and wait for them to implement new features, as opposed to having custom scripting or third-party modules. For example, advanced alarm logic or integrations outside their API scope may not be possible yet. Verkada also lacks some legacy features like *active directory integration for role-based partitioning* (they do SCIM for user provisioning, but complex role hierarchies might be limited). And if a customer needs a specific hardware configuration Verkada doesn't support (say, custom turnstile interfaces or very specialized biometric integrations), they might be out of luck because Verkada's product line is still growing (e.g., only a certain number of controller types, no native turnstile or elevator controller except basic relay workarounds). Lastly, some buyers may dislike the **heavy reliance on internet connectivity** – while controllers work offline, administration fully depends on cloud access; in highly secure or offline environments (e.g., classified facilities), this model might not be acceptable. In conclusion, Verkada excels in simplicity and integration, but those needing extreme customization or offline autonomy might find it less suitable.

6. Brivo

Overview: Brivo is a pioneer in cloud-based access control, launching one of the first SaaS access platforms in the early 2000s. Their flagship product, **Brivo Access (formerly Brivo Onair)**, is a cloud management portal paired with Brivo's hardware controllers on-premises. Brivo has a strong presence in the **mid-market and multi-site deployments** such as retail chains, property management, and small-to-medium enterprises. They also offer complementary solutions like **Brivo Mobile Pass**, **Brivo Visitor**, and even a native video integration (Brivo cams or Eagle Eye Networks, as the companies are related). Known for reliability and continuous innovation, Brivo provides a mature cloud solution with robust features and integration capabilities.

Key Features:

- **Cloud Management Platform:** Brivo Access is a fully cloud-hosted platform accessible via web browser and mobile app. It handles multi-site management very well – administrators can manage doors, schedules, and users across many properties in one interface. The system provides real-time monitoring of events, alarm triggers, and report generation. Brivo's dashboard is considered **user-friendly**, though some have found it slightly less modern in UX than newcomer interfaces. Nevertheless, it is a **proven, stable cloud platform** used by thousands of organizations. Brivo also offers a **Professional Services Portal** for integrators to manage multiple customer sites conveniently.

- **Mobile Access and Credentials:** Brivo was among the first to embrace mobile credentials with its **Brivo Mobile Pass**. This is an app that allows users to unlock doors via Bluetooth or internet command. Additionally, Brivo integrated with Apple Wallet – it offers the convenience of storing a badge in Apple Wallet for iPhone/Watch tap-to-unlock. This Apple Wallet integration is a standout, as not all systems support that yet. Brivo's mobile app also handles *administrative* tasks (for authorized admins): e.g., they can remotely unlock a door or view event logs on their phone. One limitation noted is that **mobile credentials beyond a certain number may incur extra fees** – Brivo historically included a limited number of mobile pass licenses per account, and additional ones cost extra.

- **Hardware and Infrastructure:** Brivo's controllers (like the Brivo ACS300, ACS6000) are proprietary but built on open tech (Linux-based). The controllers on-site connect to Brivo's cloud over the internet (via secure outbound connections, no inbound needed). The system uses door modules and reader interfaces that can scale from a few doors to large buildings. **Reader Compatibility:** Brivo's current hardware supports OSDP and wiegand readers – interestingly, Brivo partners with **Wavelynx** to provide reader technology. Wavelynx readers are multi-technology and allow the use of Brivo Mobile Pass (via BLE). This means if a customer leaves Brivo, those readers might need replacement since they are tied to that ecosystem. Also, some critics point out that since Brivo runs on proprietary panels, switching away from Brivo means replacing hardware.

- **Integrations and APIs:** Brivo has a **robust API ecosystem** and an **Integration Marketplace**. They integrate with **identity management systems** (Azure AD, Okta, G Suite), **CRM/Workspace apps**, and **physical security** systems. For example, Brivo can integrate with **Eagle Eye Networks VMS** to provide video linked to access events (Brivo and Eagle Eye are sister companies). They also have partnerships for **Visitor Management** (though Brivo has its own basic visitor module as well) and **Elevator control** systems. A wide range of third-party applications – including directory services, data analytics platforms, and even home automation for residential versions – can hook into Brivo. Customers and third-party developers can use Brivo's REST API to create custom solutions (such as syncing users from an HR database or triggering door events from another app).

- **Scalability:** Brivo's cloud is multi-tenant and proven to support enterprise-scale deployments. It is used in **over 20 million doors** (cumulative) according to some sources, and single deployments can involve hundreds of sites. One limitation flagged by analysts was that Brivo's interface could require more clicks than necessary for some tasks (like making user modifications across many doors). For instance, adding a user to multiple groups might involve navigating multiple tabs, whereas other systems might have a smoother workflow. But in terms of raw capacity, Brivo can handle large numbers of users and credentials. They segment enterprise features into editions – e.g., Basic, Standard, Enterprise – with advanced features (like SSO integration or increased API usage) available in higher tiers.

- **User Experience & Apps:** Brivo provides different apps: **Brivo Mobile Pass** (for end-users unlocking doors), **Brivo Access Mobile** (for admins to manage on the go), and some specialized ones like **Brivo Visitor**. One critique is that Brivo historically had multiple apps depending on use-case. For example, an end-user would use Mobile Pass, while a security manager might use a separate app for administration. Competitors like Kisi or Genea consolidate into one app. This fragmentation can confuse users or require more app maintenance, though Brivo is working to unify experiences. Additionally, Brivo's visitor management approach (Brivo Visitor) requires guests to download and sign into an app to receive their credential, which can be seen as inconvenient for one-time visitors – other systems now use QR codes or SMS links that don't require app downloads. Brivo has noted these pain points and might evolve the user experience accordingly.

- **Security & Compliance:** Brivo has strong security credentials. It is **SOC 2 Type II certified and ISO/IEC 27001:2013 certified**, demonstrating commitment to data security. They also hold a **CSA STAR Level 1** attestation for cloud security. Brivo's platform meets **GDPR** requirements and they provide documentation (DPIA support) for EU customers. They also comply with **CCPA/CPRA** in California. For payment data (though not directly relevant to access control unless using e-commerce within the system), they are **PCI-DSS compliant**. In verticals like healthcare and education, Brivo can support **HIPAA** and **FERPA** compliance needs by proper system configuration. Their hardware and systems are **NDAA compliant** (no banned Chinese components) (Source: brivo.com). Additionally, Brivo emphasizes operational security: they have a public **status page** for system uptime and redundancy across data centers. Overall, Brivo's security posture is very robust and well-documented, likely a factor in why many sensitive organizations trust their cloud.

- **Advanced Features:** Some notable features in Brivo Access include **active threat levels** (ability to change all doors to lockdown or other states with one command), **multi-factor authentication** for critical doors (requiring mobile credential plus PIN, for example), and **data dashboards** that can show occupancy trends or usage patterns for facilities. Brivo also introduced an **occupancy tracking** feature during pandemic times to monitor headcounts via access swipes. For integrators, Brivo has tools like **Brivo Snapshot** that capture and archive certain events with associated video. They also now support **Apple Watch** for unlocks via the Apple Wallet integration.

Notable Strengths: Brivo's biggest strength is its **maturity in cloud access control**. With over 20 years in the field, they have a stable, trusted platform that has been refined through extensive real-world use. Many consider Brivo the *gold standard* for cloud access in terms of reliability and security. The system provides a **robust set of features out-of-the-box**, covering most needs without requiring custom development. Brivo's integration ecosystem is rich – being able to integrate natively with **Eagle Eye cameras, alarm systems, directory services, and visitor tools** makes it a versatile choice for unified security management. The **Apple Wallet integration** for credentials is a forward-looking strength; few others have this working so seamlessly at scale. Additionally, Brivo has **scalable pricing options** and editions, making it viable for a small business with a handful of doors up to an enterprise with hundreds of sites. Another advantage is **continuous innovation**: they've kept the platform updated with things like browser-based door reader controllers (so a receptionist can unlock a door from the web), and analytics features. Also, **data ownership and privacy**: Brivo allows customers to own their data and provides exports and logs for compliance, which some more closed ecosystems don't as readily. Their longevity also means a large network of certified dealers and installers is available to support end-users globally.

Potential Drawbacks: One drawback, noted in comparisons, is that Brivo's **user interface can be less streamlined** than some newer entrants. Tasks may involve multiple screens and the UI, while functional, could feel a bit dated or complex especially in older Brivo Onair interface (the newer Brivo Access interface improved this). The **multiple apps** issue is also a drawback – managing separate mobile applications for different functions can lead to confusion and user friction. Brivo has been consolidating features into the Brivo Access platform to mitigate this. Another point is **cost considerations**: while Brivo doesn't publish pricing, it often has add-on costs for certain features or capacity. For instance, **mobile credentials beyond a small free allotment cost extra**, visitor management is an add-on module, and video integration might require Eagle Eye subscriptions. These can add up and should be planned for. Also, **hardware lock-in** is a factor: Brivo controllers only work with Brivo's cloud; if a customer ever wants to move off Brivo, the hardware would need replacing, which is a commitment to consider upfront. Some users have also cited that **support for advanced customizations** (like custom scripting or unusual use-cases) is limited – you do it Brivo's way or not at all, due to the closed cloud nature. Finally, Brivo's **visitor solution** requiring a guest to download an app is a competitive disadvantage in an era where frictionless visitor access (QR codes) is preferred. They risk falling behind if they don't introduce app-

less visitor check-in options (though integrators often solve this by adding third-party systems and integrating via API). In summary, Brivo's drawbacks are generally around UX and flexibility, rather than capability or reliability. They are working to modernize the interface, but newer players sometimes outshine them in UI elegance. Nonetheless, for many, Brivo's proven track record outweighs these concerns.

7. Avigilon Alta (Motorola Openpath)

Overview: Avigilon Alta is the rebranded **Openpath** access control solution under Motorola Solutions (which acquired Openpath in 2023). Openpath was a disruptive startup offering sleek hardware and a cloud-based, mobile-first access platform, and under Motorola it has been integrated with the Avigilon cloud ecosystem. Avigilon Alta (Openpath) focuses on **frictionless mobile access** and easy cloud management, complemented by Motorola's portfolio of video security (Avigilon Ava cameras, etc.). It's known for its beautifully designed hardware (smart readers) and a developer-friendly approach prior to acquisition. Avigilon Alta is marketed as a **premium, scalable access solution** that can work for any size organization, with particular strength in modern offices and enterprises wanting flexible, cloud-connected security.

Key Features:

- **Touchless Mobile Access:** Openpath's claim to fame was the ability for users to walk up to a door and have it unlock without needing to take out their phone. Using the Openpath app's "Wave to Unlock" feature, a user can wave their hand near the reader and, via Bluetooth/infrared, the reader detects the phone and unlocks. This provides a **hands-free entry** experience. Additionally, users can unlock via app tap or Apple Watch app. The system supports key cards and fobs as backup, but the mobile experience is primary. This is a standout for organizations wanting to ditch cards altogether. Notably, **Openpath did not support Apple Wallet or Google Wallet** as of 2025 (meaning you must use their app, not a native wallet credential) (Source: getgenea.com).

- **Cloud Platform:** Avigilon Alta's cloud software is a web portal and mobile admin app that allows full management of the system from anywhere. It includes real-time monitoring of door status, user management, and alert configurations. The interface is modern, reflecting Openpath's startup roots. It also supports **guest access links**, where admins can send a temporary link or QR code to a visitor to grant them access (without the visitor needing an app). Multi-site management is built-in, with the ability to partition by site, yet have global user directories. The cloud is globally accessible and scales on robust infrastructure (Motorola likely migrated it to their secure cloud environment).

- **Hardware & Proprietary Controllers:** The Avigilon Alta system runs on **proprietary controllers and readers** developed by Openpath. The controllers (Openpath Smart Hubs) connect to door hardware and then to cloud. They communicate outbound to the cloud and can operate offline by storing permissions locally. **Openpath Readers** are sleek, multi-technology devices that handle BLE, WiFi, and mobile authentication (and also read standard RFID cards 13.56MHz). The hardware is known for being easy to install – readers are low-profile, often using just low-voltage PoE cabling. Because it's a closed hardware ecosystem, switching to Alta requires using these controllers and readers. The benefit is that the hardware and software are tightly integrated, ensuring a seamless user experience and quick feature rollouts (e.g., firmware updates for new functions).

- **Integration with Motorola Ecosystem:** As part of Motorola, Avigilon Alta is integrated (or in process of integrating) with **Avigilon Ava Cloud Video** and **Motorola's Orchestrate and Ally platforms**. This means a user of Avigilon Alta can see video footage of access events from Avigilon cameras in the same interface, similar to Verkada's unified approach. Motorola touts "end-to-end security" – for example, integrating Openpath door alerts with Avigilon's video analytics (like opening a camera feed when a door is forced or using camera AI to verify a person's identity at access). The integration likely also extends to Motorola's radio and emergency communication systems for corporate security, although those details are evolving. Even prior to acquisition, Openpath integrated with third-party VMS like Milestone and with alarms systems for holistic security.

- **Customizable Permissions & Cloud Intelligence:** Alta provides granular role-based access control, schedules, and even zone-based restrictions. One feature Openpath had was ** occupancy tracking** – by monitoring entries/exits, the system can gauge how many people are in a space and enforce capacity if needed (important for safety or pandemic-related policies). Another is **policy-based access**, such as requiring dual-authentication on certain doors (the system supports using the app plus a second factor like biometrics or a camera intercom confirmation). Real-time alerts can be set for anomalies (door held open, multiple invalid attempts, etc.). The cloud nature also allows **over-the-air updates** that have historically added features like Lockdown from anywhere (a mobile panic button that locks all doors), or Anti-passback (though as a newer system, anti-passback might not have been initial focus, they have been adding such enterprise features over time).

- **Visitor Management & Guest Access:** Openpath didn't have a standalone visitor management app, but it made visitor access easy through its guest pass links. An admin or employee can issue a **Guest Pass** via email or SMS to a visitor, which provides a link that, when the visitor arrives, they can tap and the door will unlock for them. This bypasses the need for an app download (a convenience over Brivo's method). Additionally, Openpath integrates with popular visitor systems like Envoy – when a visitor signs in on an iPad, Envoy can trigger Openpath to send them a mobile credential for the duration of their visit. This integration capability for visitor management is a strength.

- **Third-Party Integrations & API:** Openpath was built with openness in mind (despite proprietary hardware). It has a well-documented **REST API** and supports **webhooks**, enabling integration with HR databases, identity providers, and other services. Out-of-the-box integrations include **Okta**, **Azure AD**, **Google Workspace** for directory sync, **Slack** for alert notifications, and various analytics platforms. They also integrate with **SAML SSO** for single sign-on to the admin dashboard. Another integration is with **IFTTT or Zapier** – enabling creative automations like turning on lights when someone badges in, etc., reflecting a tech-forward approach.

- **Compliance & Security:** Motorola has ensured Avigilon Alta meets enterprise security standards. It has achieved **SOC 2 Type II** and **ISO 27001** certifications as indicated by Motorola's trust center. It also adheres to GDPR for data privacy (with data hosting options in-region). Openpath's hardware was **UL 294 certified** for access control safety, and NDAA compliant. They use end-to-end encryption and offer features like **"Triple Unlock"** (three methods of communication – BLE, WiFi, cellular – to maximize chances a door opens even if one channel is down). While Apple Wallet is not integrated, security of their mobile credential is high, using phone's biometric unlock for the app and secure cloud token exchanges. Post-acquisition, Motorola has likely integrated the product into its FIPS 140-2 validated cryptography processes as well. As a side note, Openpath's cloud was hosted on Google Cloud Platform, known for reliable infrastructure, but under Motorola some backend may shift.

- **Pricing:** Openpath (Avigilon Alta) is sold via integrators and partners. It typically charges for hardware and a subscription per door per year for cloud access. While not public, pricing was competitive with other premium cloud offerings. They often pitched ROI in eliminating keycards (because mobile is included unlimited). One important note: Openpath does **not charge per mobile credential** – any number of users can use the system at no extra cost, which is a differentiator from some older models. This encourages broad adoption of mobile access among employees without worry of incremental fees.

Notable Strengths: Avigilon Alta (Openpath) is particularly praised for its **user experience** – from the sleekness of tapping your phone or waving to unlock, to the clean admin interface. It provides a very modern experience that aligns with the expectations of tech companies and forward-thinking businesses. The **frictionless access** feature (Wave to Unlock) is a big plus for convenience and hygiene (a selling point during COVID). Integration with the **Motorola ecosystem** now means a strong combined solution of access + video + intercom, with Motorola's reliability behind it. Another strength is the **speed of innovation**: as a startup-born product, Openpath pushed updates frequently and added capabilities like lockdown commands, occupancy counting, etc., and that culture can continue under Motorola. The hardware design is also a plus: the controllers are smart and the readers are attractive (some companies choose Alta just because the readers look nicer in their lobbies than older clunky readers). **Scalability and remote management** are inherent strengths as a cloud system – multi-site management is easy and global changes are real-time. The ability for administrators to use a **mobile app for admin** tasks (Openpath app allows admins to do quick actions and see events) is useful. In terms of **integrations**, Alta was among the best in class, supporting a variety of workplace tools (e.g., it integrates with **Office 365 and G Suite calendars** so if a meeting room is reserved, it can grant access during that slot – a unique integration for office management). Lastly, being part of Motorola gives it financial stability and support, alleviating any previous concerns some had about startup longevity when it was Openpath standalone.

Potential Drawbacks: One drawback noted in competitor analyses was the lack of Apple/Google wallet support (Source: getgenea.com) – requiring use of their app might be a barrier for some users who prefer native wallet badges. There's also the **proprietary hardware lock-in**: you must use their controllers and readers, which could be expensive to swap in initially (though they try to reuse existing wiring and locks). Some larger enterprises might find a few feature gaps compared to incumbents: for example, **no native offline mode for sites with no internet** – it's cloud-dependent (though you can run it on cellular backup). Also, **no built-in alarm monitoring**; while Alta can integrate with alarm systems, it doesn't have its own intrusion system (Verkada does, Brivo integrates tightly with alarm.com). Another consideration is that, under Motorola branding, some worry if the **openness will remain** – historically Openpath was quite open API, but big companies sometimes turn products more closed; however, given Motorola's track record, they likely keep APIs. Additionally, some users reported that while the system is great when all is well, **troubleshooting network issues or hardware issues** can be challenging since it's dependent on cloud – e.g., if a controller goes offline, you rely on remote support or on-site fixes with less local override compared to older systems (though there is a failsafe physical key option for doors if needed). Cost-wise, Alta is a premium solution; hardware can be pricier than generic Mercury panels, and the subscription per door is significant (though comparable to Kisi or Brivo's enterprise tiers). Lastly, as with any acquisition, there could be **transitional hiccups** – some customers worried about support changes or strategy changes under Motorola (e.g., Motorola merging Alta with other cloud offerings like Ava – but so far they kept "Alta" as their cloud brand, separate from on-prem Avigilon Unity line). All considered, Avigilon Alta's drawbacks are relatively minor and typical of a cloud, proprietary system – they revolve around ensuring it fits the organization's IT preferences (proprietary vs open, app vs wallet, etc.) and budgeting for a high-end solution.

8. Dormakaba

Overview: Dormakaba is a global leader in locks, door hardware, and physical access solutions. In access control, Dormakaba offers both **enterprise systems** (like their exos and MATRIX software, Keyscan line in North America) and **cloud-based solutions** (such as Dormakaba exivo in Europe). Dormakaba's strength lies in its extensive hardware portfolio – from electronic locks and readers to revolving doors and turnstiles – and its presence in verticals like hospitality, where it's a dominant provider of hotel door locks. As a commercial access control solution, Dormakaba provides end-to-end coverage: they manufacture the locks/door devices and the software to manage them. Dormakaba's offerings are often tailored to specific needs (e.g., their wireless lock systems for universities, or keyless systems for co-working). The company's approach emphasizes **security, durability, and integration of mechanical and electronic access**.

Key Features:

- **Integrated Hardware Solutions:** Dormakaba provides a **wide range of access hardware** that can all tie into their systems. This includes traditional wall-mounted card readers, wireless electronic door locks (both RFID and BLE-enabled, often branded as Orbis or similar for standalone locks), **keypad locks**, and high-security cylinders. They also offer entrance systems like **turnstiles, speed gates, and revolving doors** that integrate with their access control. The benefit is a one-vendor solution for everything from your parking gate to your server room door. For example, Dormakaba's wireless locks can be managed online through their software, reducing wiring in retrofits.

- **Software Platforms:** Dormakaba's enterprise software like **Exos** (commonly used in EMEA) or **Keyscan Aurora** (popular in Americas due to Dormakaba's Keyscan acquisition) provide robust on-premises access management. These systems allow client-server architecture, role-based permissions, schedules, and integration with video/alarms. Exos is highly scalable, used in large institutions and supports multi-tenant scenarios (like multi-tenant office buildings). Dormakaba also has **mobile apps for administration** and user functions in some offerings, though historically they have been more PC-client oriented. For SMB and cloud, Dormakaba's **exivo** is a cloud platform where integrators can manage access for multiple customers (particularly marketed in Europe for small facilities, allowing remote management by a service provider). It's worth noting that Dormakaba's portfolio is broad and somewhat fragmented: different regions use different primary software (e.g., in the US, the Keyscan Aurora and Smartspace software, in EU exos and exivo, in hospitality the Saflok/Ilco systems).

- **Mobile Credentials:** Dormakaba supports mobile access through BLE in many of its newer locks and readers. For instance, their Saflok hotel systems allow guests to use a smartphone key via BLE. In commercial systems, Dormakaba has mobile solutions (some of which leverage cloud credentials or third-party platforms). For example, Dormakaba partnered with **Legic** and others for secure mobile credentials. However, the adoption of mobile in general security (outside hospitality) has been a bit slower for them relative to pure tech companies. It's an available feature, but not as central in marketing as with Kisi or Openpath. That said, Dormakaba did introduce features like **digital credential provisioning** for remote sites and **Bluetooth readers** that can read mobile keys or Apple Wallet keys for hotel use.

- **Visitor Management & High-Security Modules:** Dormakaba's enterprise systems often include **visitor registration modules** or integrate easily with third-party visitor systems. They also cater to high-security needs with modules like **badging (ID card printing)**, **guard tour**, and specialized workflows (e.g., handling key cabinets, integrating with physical key systems – a nod to their mechanical keying background). They emphasize compliance features like **audit trails** and even **biometric integration** for areas needing two-factor authentication (Dormakaba acquired Stallings, a biometric reader company, years back). For example, their systems can require fingerprint or iris verification in addition to card swipe for certain doors – useful in labs or data centers.

- **Scalability & Enterprise Focus:** Dormakaba access systems can scale to thousands of doors and users. They are used in **airports, universities, healthcare complexes**, etc., where integration of many door types (wired and wireless) is needed. For instance, a campus might use dormakaba wireless locks on dorm rooms, hardwired readers on main entrances, and turnstiles at the gym – all managed under one umbrella software. The systems are typically integrated with **enterprise systems like SAP or HR databases**, syncing user statuses. Dormakaba's exos has features for **contractor management** and **visitor self-registration**, showing an enterprise orientation.

- **Third-Party Integrations:** Dormakaba's software can integrate with **building management systems**, **fire alarm systems** (e.g., to unlock doors on fire alarms), and **elevator controls** (they have their own relay boards or integrate with OTIS/Schindler, etc.). They also offer **API/SDKs** for their products – for instance, Keyscan Aurora has SDK for custom integrations. In the PropTech space, Dormakaba works with companies like **Altus and Spaceti** to integrate access data into workspace management. And, because of their hospitality focus, they integrate with **Property Management Systems (PMS)** like Oracle Opera for hotel guest key issuance.

- **Compliance & Certifications:** As a large company, Dormakaba meets global standards. They have **ISO 27001** certifications for their information security in some divisions (Source: dormakaba.com). They likely follow SOC 2 internally for cloud offerings (exivo, etc.), though not heavily publicized. Dormakaba hardware often meets strict safety and security certifications: **UL294, CE**, etc., and many products are **BSI (German) or VdS** certified for high security. They also emphasize **privacy compliance** for cloud services. Dormakaba uses secure encryption for credentials (their RFID cards typically use secure MIFARE DESFire or Legic advant). They also comply with data protection laws as needed – for example, exivo being hosted in Swiss data centers for European clients, aligning with GDPR. An interesting compliance note: Dormakaba provides **TÜV-certified** systems for certain government applications, reflecting a deep trust in their security.

- **Industry Solutions:** Dormakaba highly customizes solutions for industries. In **hospitality**, their access system ties to hotel check-in, with features like guest room access scheduling, master keys for staff with tracking, etc. In **commercial real estate**, they offer multi-tenant access control that integrates with tenant directories and possibly billing systems. In **education**, they have solutions for managing student housing access, integrating with student databases. In **healthcare**, they integrate with infant security systems or pharmacy dispensing units. Essentially, beyond generic features, Dormakaba provides tailored modules or partnerships to address specific industry needs (like lockdown function for schools, or anti-ligature locks for behavioral health facilities). This customization is a key strength of their offerings.

Notable Strengths: Dormakaba's strongest asset is its **comprehensive hardware and global expertise**. Few companies can offer everything from a door closer to an electronic access management software – Dormakaba can. This means a very **seamless integration of physical door hardware with electronic control**: for example, they ensure their locks work smoothly with their readers in terms of mechanical reliability. Their solutions are **battle-tested in high-traffic environments** (airports, big universities). Dormakaba is also at the forefront of **wireless lock tech**; they and Assa Abloy largely pioneered wireless, battery-operated locks that report to an access system, which is crucial for retrofitting older buildings (cheaper than running wires to every interior door). Moreover, their **experience in hospitality** gives them a user-experience edge for certain applications – e.g., managing temporary guest access is something they do millions of times daily in hotels. Another strength is **regional support and presence**: being global, they have local offices or partners in almost every country, which is reassuring for multinational companies that want standardized systems. Dormakaba also stands out in **combining security with convenience** – their systems tend to have lots of options to fine-tune (like you can define very specific access rules, holidays, etc.) and integrate mechanical key systems for a holistic approach (like tying physical master key check-outs into the electronic audit trail). The company also invests in R&D around **new**

tech: e.g., they have explored using **smart keys**, **mobile keys**, and even **blockchain** for access credentials in concept. Lastly, Dormakaba's financial stability and longevity (they result from a merger of Dorma and Kaba, each over a century old) give confidence to large clients that the system will be supported for years and is not an upstart product.

Potential Drawbacks: One drawback can be the **complexity and siloed nature** of their portfolio. Because they have multiple product lines (Keyscan, exos, exivo, Saflok, etc.), it's not always clear which is "the Dormakaba system" one should choose, and they aren't all unified. A customer might end up with different Dormakaba platforms for different use cases (e.g., separate hotel system and corporate office system not talking to each other). This fragmentation can also slow down innovation; a smaller competitor might update faster than a large company coordinating multiple lines. In terms of software user-friendliness, Dormakaba's interfaces have historically been **more utilitarian** – they work well but may look dated or require more training compared to slick new cloud UIs. Also, Dormakaba has been **slower to fully embrace cloud globally**; while exivo is a cloud product, its uptake is limited to certain regions and project sizes. Many Dormakaba deployments are still on-premises, which for some is fine, but others may see that as lagging behind the cloud trend. Another drawback is **cost**: Dormakaba gear is premium quality, and often priced accordingly. The total cost of a Dormakaba integrated solution (with wireless locks, etc.) can be high, although sometimes offset by savings in labor (wireless means less cabling cost). Additionally, **integration with third-party systems** might be less out-of-the-box than some newcomers – e.g., an API exists, but you may need Dormakaba's help or a dealer to script something, whereas a modern SaaS might have plug-and-play connectors. The **mobile experience** for end-users isn't as seamless as ones built mobile-first (Openpath, Kisi, etc.), though they do support it. Another subtle drawback: being a hardware-oriented firm, their **software support model** is often through dealers/integrators, so response times or innovation might depend on that chain, whereas a SaaS company directly supports the end-customer swiftly. Finally, while Dormakaba covers basics like SOC2 via ISO certs, they might not market it strongly – some IT buyers might not immediately see Dormakaba as a "software company" and be cautious about cloud security, though the trust is likely well-placed given their certifications (Source: dormakaba.com). In essence, Dormakaba's drawbacks are typical for a large established firm: potentially less nimble, sometimes less user-focused on the software side, and a bit complex to navigate, but none of these detract from their core strength in delivering solid, integrated access control.

9. Salto Systems

Overview: Salto Systems is a Spanish manufacturer renowned for its innovative **wireless locking technology** and keyless access solutions. Salto's products are used in a range of environments from offices and co-working spaces to hotels and large campuses. Salto's hallmark is the **ability to mix and match offline, wireless, and wired access points** in one system. They offer a cloud-based platform called **Salto KS (Keys as a Service)** for managing locks remotely, as well as on-premises systems like **Salto Space** for more localized control. Salto pioneered the concept of the "virtual network" for locks (SVN), where stand-alone locks can exchange data via user credentials – a unique approach that predates IoT but achieved many of its benefits. This allows a highly scalable system with minimal wiring. Salto's focus is on **flexibility and user-friendly keyless experiences**.

Key Features:

- **Wireless & Smart Locks:** Salto's core hardware includes a wide variety of **electronic lock formats** – from cylindrical locks, escutcheons, mortise locks, padlocks, to wall readers for elevators or parking gates. Most of these can operate wirelessly (via BLE/Zigbee) or standalone (offline). Their locks typically store access permissions locally and make decisions at the door. Salto's **SVN (Salto Virtual Network)** technology allows offline locks to update and receive updates through user credentials: for instance, a user's card can pick up a blacklist or battery status from one online reader and deliver it to offline locks on other doors during normal use, achieving distributed intelligence. Additionally, Salto has **online wireless locks** that communicate in real-time through gateways, giving live audit trails and instant remote unlock capabilities. This breadth of lock formats makes Salto ideal for retrofits in older buildings or places where wiring every door is impractical (like historic buildings, or covering dozens of doors in a school dorm).

- **Cloud Platform (Salto KS):** Salto KS is a cloud-based system aimed at giving customers remote access management via web or mobile app. It's particularly popular in co-working spaces, multi-tenant offices, and small businesses. With KS, administrators can issue digital keys instantly, revoke access in real-time, and monitor events from anywhere. The mobile app for Salto KS allows door unlocking, meaning users can use their smartphone (with the app) to unlock Salto BLE-enabled locks. There's also integration of **cloud API** for connecting Salto KS to other apps (like scheduling software or member management in co-workings). Key features of Salto KS include **remote management of multiple sites**, **sharing digital keys via SMS/email**, **real-time alerts**, and a sleek interface that doesn't require deep technical knowledge to operate. Scalability is a strong point – Salto KS can manage unlimited locks across different locations as needed, since all is in the cloud.

- **On-Premises System (Salto Space):** For enterprises that prefer local control, Salto Space (with ProAccess SPACE software) is their on-prem management tool. It allows more customization, such as **defining complex access groups, time zones, and holidays**. It supports the mixing of online and offline locks. With Space, Salto offers features like **"JustIN Mobile"** – their mobile key technology – even for on-prem setups (the keys are distributed via a cloud service even if the management is on-prem). It also provides **integrations** into PMS (Property Management Systems) for hotels, or access to an **API/SDK** for custom integrations on site. The on-prem solution requires setting up servers and often is delivered by Salto's integrator partners; it's robust and used in large institutions (corporate HQs, universities, etc.).

- **Mobile Access:** Salto has been strong in mobile access, especially with **JustIN Mobile**. Users can receive a mobile key on their smartphone through the JustIN Mobile app, which uses BLE to unlock locks. This is heavily used in hotels now (guests receive their room key on phone), and increasingly in offices. The mobile keys are encrypted and can work even offline once downloaded (they contain the access rights). In Salto KS, mobile unlocks are done via the KS app, similarly. Additionally, Salto has implemented features like **Tap to Unlock via NFC** on Android, and was exploring Apple Wallet keys (they

might support it for some hospitality solutions or will soon, since Apple opened that up to third parties like Assa Abloy and Dormakaba for hotels). Salto's approach is to offer multiple credential options: you can use cards (MIFARE, DESFire, etc.), **fobs, bracelets, NFC stickers**, PIN codes (they have locks with keypads), and mobile apps – making it very flexible for the end user.

- **Third-Party Integrations:** Through Salto KS's API and Salto Space's integration capabilities, Salto integrates with many platforms. In co-working, Salto KS integrates with **platforms like Office RnD, Nexudus** (membership management), enabling space managers to automate access when a new member signs up. They also integrate with **Google Workspace and Microsoft 365** to some extent (for instance, using calendar to open meeting rooms). For hotels, Salto works with all major PMS systems to automatically assign room access on check-in and revoke on check-out. Salto has integrated with **elevator systems** to allow use of the same credential in elevators (with restricted floor access). Also, Salto has partnerships for **visitor management** – one can send a JustIN Mobile key to a visitor's phone ahead of time, for example. Their API allows retrieving logs and managing users from external programs. For instance, a student information system at a university could be linked so that when a student enrolls, a Salto credential is created, etc. Salto also announced integration with **Cisco Meraki cameras** for an integrated security solution (Meraki logs could tie to door events). While not as publicly advertised as some, these integrations make Salto quite adaptable.

- **Security & Compliance:** Salto's technology uses high-security encryption (their smartcards use 128-bit AES on DESFire, etc., and mobile keys are similarly secured). The ISO 27001 certification for their cloud operations confirms they maintain strong infosec practices. They completed a **SOC 2 Type II audit** as mentioned in one of their help center articles, demonstrating commitment to data security and processes. Salto KS cloud data is often hosted on AWS in secure zones, and they comply with GDPR by design (Europe-based, they are mindful of privacy). Their hardware is **certified** – e.g., many locks are **EN rated for fire and safety**, and some are **BHMA certified** in the US for durability. One unique aspect: since many Salto locks are battery powered, they include safety measures like warning when battery is low long before it dies (so you can replace it). They also allow emergency overrides – mechanical keyways or 9V jump start nodes – to ensure one isn't locked out due to power issues. These aren't security features per se, but important operational safety features. Additionally, Salto's system can be set to require **multi-factor at the lock** (like pin + card on certain locks that have keypads for higher security areas). And they are taking compliance seriously by renewing ISO27001 and aligning with standards like **Common Criteria** in some products (for government use cases requiring certified equipment).

Notable Strengths: Salto's primary strength is its **versatile hardware and hybrid network**. In an environment like a university or modern office, Salto can put electronic access on *every door*, not just perimeter ones, because you don't need to wire every door – this is a huge advantage in expanding electronic access control where it was previously cost-prohibitive. The **user experience** is also a focus: their locks are often stylish (they have designer series locks to match decor), and things like the ability to use a wristband at a gym or a phone at an office gives users convenient options. **Scalability** is proven; Salto installations can run into thousands of locks (e.g., large university housing systems). Another strength is **offline capability** – because locks can work standalone and cache data, a temporary network outage or cloud outage won't immediately compromise local access; things will sync later. For Salto KS, the ease of inviting a user and instantly granting access via cloud is a big plus (like sending digital keys remotely). Salto's deep industry presence means they understand and have features for specific scenarios: e.g., their occupancy feature in KS that does **real-time occupancy tracking** can help measure space utilization (for co-work or offices). They also introduced an **"Emergency Override"** mode where doors can be configured to fail open or lock on signal from a fire system, etc. The **community around Salto** – integrators worldwide – is strong, so support and knowledge are widespread. Lastly, Salto is known for being **innovative**: they were one of the first with smartphone keys, and they keep pushing (e.g., recently exploring BLE/WiFi combo locks, cloud-to-cloud integrations, etc.). They also care about **data** – KS has analytics and reporting that can show usage patterns, helping businesses optimize how spaces are used.

Potential Drawbacks: One drawback is the **reliance on proprietary locks** – if you go Salto, you use their locks and cylinders. While they integrate third-party readers, their full benefit is in using Salto locks. If one wanted to mix Salto with, say, another vendor's locks or controllers, that's not really possible at the software level (though some have done setups where Salto is for interior locks and another system for perimeter and they just sync users between them – but that's clunky). Another is that **Salto KS, being cloud, depends on subscription**, which some traditional customers balk at (they'd prefer a one-time purchase; Salto does give that option with Space though). For Salto KS specifically, some advanced features of enterprise systems might be missing – e.g., intricate zone anti-passback, or integration with enterprise IT systems might not be as broad (though it covers a lot through API). Also, **mobile keys require the app** – not a huge deal, but some prefer the native wallet approach, which is not fully utilized outside hospitality yet by Salto (though they likely will follow if industry does). While Salto's multi-technology approach is a strength, it can also make the system **complex to administer** if you have a mix of offline and online – you need to manage battery levels, understand how data flows through the virtual network (some learning curve for those not familiar). Their offline mechanism (SVN) while clever, means things like if someone's access is revoked, they might still have access until they either present their card to an online updater or the lock has a timeout for cache – thus immediate revocation is guaranteed only on online locks. They mitigate with short cache times and encouraging people to use mobile (which updates instantly if online) or the practice of updating cards frequently, but it's a consideration – **truly real-time control** is on the wireless online locks; for pure offline, there's a slight delay by nature. In terms of UI, Salto KS is good, but the on-prem software historically was seen as less modern interface (improving though). Also, **cost**: Salto locks are not cheap; each door lock could be several hundred dollars plus the software/license costs. But one could argue wiring and labor saved makes up for it. Lastly, some have noted that **support for Salto can vary by region** – in some areas, you must rely heavily on the local dealer for support (which might be great or might be mediocre) as Salto itself is manufacturer and doesn't support end-users directly as much; this is typical in the lock industry. Summarily, Salto's drawbacks are tied to its unique approach (offline vs online complexity, proprietary nature) and ensuring the user's operational processes adapt to that (like keeping up with battery changes, etc.), but these are manageable with best practices.

10. Honeywell Commercial Security

Overview: Honeywell is a major conglomerate with a strong security division offering access control, video surveillance, and intrusion systems. In access control, Honeywell's flagship enterprise offerings include **Pro-Watch Security Suite** and **WIN-PAK** (for SMB), as well as *MaxPro Cloud* for a hosted approach. Honeywell's systems are widely used in **large-scale projects such as airports, government facilities, and corporate campuses**, as well as mid-sized commercial buildings. Historically, Honeywell's security products came through acquisition (e.g., Northern Computers/Win-Pak, and later the Pro-Watch enterprise platform, which integrates with Honeywell's own and third-party hardware). Honeywell's strength is in providing a **comprehensive, integrated security solution** – they often tie access control with their **video management (e.g., MaxPro VMS) and building automation systems**. They are known for robust hardware and an established partner network.

Key Features:

- **Panel-Based Access Systems:** Honeywell's traditional approach uses control panels (like N1000, NS2, or newer modular controllers) that handle door connectivity, connected to either on-prem server or cloud. **WIN-PAK** is a software for small to medium installations, supporting up to dozens of doors and users in the tens of thousands. **Pro-Watch** is the enterprise software, scaling to hundreds of sites and thousands of doors. These systems offer real-time monitoring, alarm/event management, and reporting. They support **generic (Mercury-based) door controllers** in newer versions (Honeywell's own OEM hardware and HID Mercury boards), ensuring flexibility and easy expansion. Honeywell panels are quite standard in wiring and functionality, making them a known quantity for installers.

- **Integration & Versatility:** Honeywell's platform is often described as **versatile but "piecemeal"** by some, meaning they offer many pieces you can combine for a solution. For example, video integration: Pro-Watch can integrate with Honeywell's **MaxPro NVRs** or DVM (Digital Video Manager) to tie video with access events. They also can integrate with **Honeywell's intrusion panels** (like Galaxy or VISTA series) for arming/disarming via access events. The system provides features like **alarm graphics maps**, muster reporting, visitor enrollment, and ID badge printing natively. They have a native **visitor management** module and even a **lobby kiosk** option – beneficial for large complexes.

- **Web & Mobile Interfaces:** Historically, one critique was that Honeywell lacked a slick web or mobile interface for management (older WIN-PAK was Windows-only UI). However, newer offerings like **Pro-Watch 5.0 and WIN-PAK CS** have introduced web client components and mobile apps (like *Honeywell Secure* app for situational awareness (Source: play.google.com), albeit that might be more focused on video/alarm). They've been bridging that gap with **MaxPro Cloud** – a platform where smaller panels (like MB-series controllers) connect to cloud and allow remote management of both access and video. This is geared toward multi-site small businesses or franchises to manage security remotely. That said, their core enterprise stuff still often uses thick client software for the full feature set, which can be less accessible remotely.

- **Scalability & Enterprise Features:** Honeywell Pro-Watch is used in some of the most demanding environments – e.g., airports where you might have tens of thousands of cardholders, integrations with **government PIV badges** for federal sites, and requirements for high availability. Pro-Watch supports redundant servers, database clustering, and can interface with **Honeywell's Enterprise Buildings Integrator (EBI)** for connecting to HVAC, fire, etc. They emphasize **"enterprise-grade security"** and indeed have features like encryption at all levels, secure credential standards (they support OSDP readers, newer credential tech). **Credential management** in Pro-Watch can be advanced – linking to corporate directories, managing expiring clearances, etc. Also, their systems handle **maps of live floor plans** where you can see door status and alarms graphically, which is useful for 24/7 security control centers.

- **No-Cloud or Cloud-Optional:** Some customers specifically choose Honeywell because they want an on-premise system with no dependence on cloud or outside connectivity (e.g., government or industrial sectors). Honeywell fulfills that with Pro-Watch/WinPak – which can be entirely self-contained, with integration to onsite systems. At the same time, for those who want cloud convenience (like integrators offering managed services), Honeywell offers **WIN-PAK CS (central station) edition** or MaxPro Cloud which allow remote management by a dealer or user. This flexibility means Honeywell can cater to both preferences. However, one downside historically is that **Honeywell's cloud lags behind** dedicated cloud competitors in simplicity and user experience (MaxPro Cloud was initially more video-focused and basic for access).

- **Third-Party Hardware & Software Integration:** Honeywell works with multiple hardware lines. They have their own **OmniAssure** readers for secure credentials, but also support HID, MIFARE, etc. The systems can use Mercury boards which means you could potentially swap software to another Mercury-compatible platform if needed (though Honeywell tries to keep you in ecosystem). On software integration, they may not have as open an API as newer SaaS, but Pro-Watch does have an SDK and connectors to systems like **Lenel for data exchange** (for large enterprise unifications). They historically lack direct integrations to things like HR systems out-of-box (which newer cloud systems tout), but integrators often do custom solutions for that or use import tools. Notably, Honeywell's focus on **compliance** yields built-in features rather than requiring integration: e.g., **compliance reports for SOX or TSA regulations** can be generated directly in Pro-Watch, something a finance or aviation customer might need.

Notable Strengths: Honeywell's access control is battle-hardened for large, **mission-critical installations**. Their systems handle **complex scenarios** – multiple sites, multi-factor authentication (they support biometric readers natively, and things like requiring two people to present credentials to open a door, etc.), and deep integration with other security systems. The **breadth of solution** from one company is a strength: they can provide the **cameras (30 Series, etc.), the recorder (MaxPro), the access system (Pro-Watch), and even the alarm system**, all tied together. Many security directors like a one-stop integrated solution. Honeywell's gear is also known for **longevity and support** – some Win-Pak systems have run for decades; Honeywell provides long-term support cycles (though sometimes slow to upgrade features). The **customer support infrastructure** via Honeywell and its certified dealers is strong globally.

Another strength is **vertical experience**: they have dedicated solutions/teams for **airport security, federal projects, healthcare** (with things like infant abduction systems integrated), etc. They know how to meet high compliance standards (for instance, Pro-Watch is FICAM compliant for U.S. federal standards out of the box). **Stability and reliability** of Honeywell systems are often cited; they may not be flashy, but they are dependable – this is crucial for facilities that can't afford downtime (like an airport can't have its access control offline – Honeywell systems are built to be up 24/7 with failovers). Also, **backwards compatibility** – Honeywell often supports older hardware in newer software generations, easing upgrades. Honeywell also leads in some **specialized tech**: e.g., they have an intelligent **smartcard printer/encoder** solution that ties into Pro-Watch so you manage badges seamlessly. And their **global presence** means local language support, compliance with local regulations (like GDPR, they have modules to help anonymize personal data in logs when needed), etc.

Potential Drawbacks: Despite offering cloud options, Honeywell has been perceived as **lagging in cloud-first innovation**. As Genea's blog noted, it's somewhat **"piecemeal"** with older architecture in parts. For example, no single unified mobile app experience for everything – some tasks require the thick client, and mobile use is limited (lack of a true mobile credential platform, though they have hardware capability, the management of it isn't as seamless as some new players). Indeed, Genea pointed out **"no native mobile access platform – can't control through smartphone"** as a drawback (as of that writing). So, user-friendliness suffers; small organizations might find Honeywell overly complex to self-manage and would lean on an integrator. Another drawback is that **Honeywell's focus on large projects** sometimes means smaller customers feel underserviced unless they go through a dealer who's excited about cloud services. Also, **cost** can be an issue: Honeywell enterprise solutions are known to be on the expensive side (proprietary software licensing, annual support contracts, high-end hardware). And often **pricing is not transparent** – you have to go through a quote process. Another common complaint is **customer support bureaucracy** – as a big company, things can move slowly. Also, because Honeywell does so much (from thermostats to aerospace), sometimes customers worry if a specific product line (like Win-Pak) is getting enough R&D attention; Honeywell did discontinue some smaller lines in past (like the NetAXS cloud attempt in early 2010s got folded). But given their ongoing updates to Pro-Watch/MaxPro, they're invested in security. Lastly, **fewer modern integration capabilities** – for example, direct integration to Slack or Teams for door events isn't a standard feature (though via some connected services it could be done). They also generally **lack native directory (Okta/Azure) integration** for user provisioning – meaning it might rely on manual import or custom work, which is less appealing in an automated world. In summary, Honeywell's drawbacks revolve around *user experience (older UI, no one-app-for-all), agility (less quick to adopt new tech unless market-proven), and cost/complexity (enterprise-level overhead for potentially simpler needs)*. For a tech-savvy client wanting immediate slick interfaces and rapid feature updates, Honeywell might feel stodgy. However, for those prioritizing proven reliability and deep integration in a complex environment, those drawbacks may be acceptable trade-offs.

Comparative Feature Matrix Table

The table below compares all ten solutions across key features and criteria:

FEATURE / CRITERIA	KISI	JCI (C•CURE)	ADT	ACRE (FEENICS)	VERKADA	BRIVO	AVIGILON ALTA	DORMAKABA
Cloud-Based Management	Yes	Hybrid (Cloud option)	Yes (via ADT apps)	Yes	Yes (Source: verkada.com)	Yes	Yes	Partial (exivo on-prem too)
Mobile Access (App/Wallet)	Yes (App + Apple Wallet)	Partial (HID Mobile via readers)	Yes (Mobile app & SMS links)	Limited (no native; HID via Mercury)	Yes (App, Bluetooth touchless)	Yes (Mobile Pass app; Apple Wallet)	Yes (Openpath app; no Apple Wallet) (Source: getgenea.com)	Yes (JustIN m BLE locks)
Proprietary vs Open Hardware	Proprietary controllers; open API	Mix (proprietary panels; Mercury support)	Uses various (often Mercury/HID)	Open (Mercury HW)	Proprietary (Verkada AC controllers)	Proprietary (Brivo panels; Wavelynx readers)	Proprietary (Alta controllers/readers) (Source: getgenea.com)	Proprietary lo some Mercur integration
Scalability (Doors & Sites)	High (SMB to enterprise global)	Very High (enterprise campuses)	High (with ADT Commercial for large projects)	High (cloud scales; Mercury-based)	High (10 to 10,000 doors)	High (multi-site cloud)	High (cloud multi-site)	High (enterpr hotels)
Visitor Management	Basic (QR codes, links)	Yes (Native module in C•CURE)	Integrated with alarms/intercom (ADT offers solutions)	Yes (Native VM & kiosk)	Verkada Guest (built-in visitor)	Yes (Brivo Visitor; app required)	Via guest links or Envoy integration	Yes (has visit options, espe hotels)
Real-Time Alerts & Logs	Yes (live logs, custom alerts)	Yes (24/7 monitoring consoles)	Yes (alerts through app/SMS)	Yes (cloud dashboard + reports)	Yes (instant alerts + video context)	Yes (alerts, robust reporting)	Yes (real-time cloud events)	Yes (enterpris logging)
Custom Permissions/Roles	Yes (group-based, schedules)	Yes (very granular, enterprise RBAC)	Yes (flexible via customization)	Yes (groups, roles, time-based)	Yes (user groups, SCIM for roles)	Yes (multi-level admin roles)	Yes (roles & cloud admin roles)	Yes (fine-grai software)
Remote Unlock Capabilities	Yes (via cloud web/app)	Partial (via thick client or new web module)	Yes (ADT app or call center)	Yes (cloud or mobile admin)	Yes (Command app/web)	Yes (web portal & mobile admin)	Yes (cloud dashboard or app)	Yes (for onlin offline via up
3rd-Party Integrations	Yes (20+ integrations: AD, Slack, etc.)	Yes (video, alarms, identity via SDK)	Yes (security ecosystem, custom via ADT integrator)	Yes (Workday HR, Okta, etc.)	Yes (API, webhooks, SCIM, integrates video)	Yes (Open API, Eagle Eye VMS, Envoy)	Yes (Okta, Envoy, G Suite, Slack)	Yes (PMS for BMS, etc.)
Security Certifications	SOC 2, ISO 27001, GDPR	SOC2-ready (cloud on AWS), FIPS 201	– (Relies on underlying providers; ADT monitoring UL cert.)	– (Not public, but AWS-based; Mercury HW)	SOC 2, ISO 27001/17/18	SOC 2 Type II, ISO 27001	SOC 2, ISO 27001+ (Motorola trust center)	ISO 27001 for (Source: dormakabagr

FEATURE / CRITERIA	KISI	JCI (C•CURE)	ADT	ACRE (FEENICS)	VERKADA	BRIVO	AVIGILON ALTA	DORMAKABA
Pricing Transparency	High – published range (hardware & subscription)	Low – quote-based (enterprise licensing)	Medium – bundles with monitoring, quote-based	Medium – through dealers; subscription pricing available	Medium – standardized pricing via reps (TCO includes license per device)	Medium – through dealers; known to charge for some extras	Medium – via integrators, known pricing tiers but not public	Low – dealer varies by proj
Industry-Specific Solutions	Yes (coworking, fitness, offices) (Source: getkisi.com)	Yes (government, enterprise, aviation)	Yes (retail, SMB, multi-site franchises)	Not explicit, but enterprise focus (tech, CRE)	Yes (education, retail, government use cases showcased)	Yes (multi-family, commercial, churches, etc.)	Yes (office, multifamily, tech campuses)	Yes (hospitali airports, etc.)

Table Notes: "Partial" indicates the feature is available but with some limitations or via third-party means. A blank/"–" means not explicitly applicable or not prominently advertised. Each solution's capabilities are cited from the sources: for example, Kisi's integration and mobile strengths, Johnson Controls' cloud compliance, Brivo's certifications, etc. This matrix highlights how newer cloud solutions (Kisi, Verkada, Brivo, Openpath) excel in mobile friendliness and simplicity, whereas traditional systems (Johnson, Honeywell) shine in large-scale, on-premises integration but are adapting to cloud expectations. Mid-range players (ACRE's Feenics, Dormakaba, Salto) offer specialized flexibility – Mercury openness, wireless locks – filling unique needs in the market.

Conclusion and Recommendations by Use Case

In 2025, the landscape of commercial access control solutions ranges from cloud-native upstarts to venerable enterprise platforms. The "best" choice depends heavily on an organization's size, industry, and specific security requirements. Below, we conclude with tailored recommendations for various common use cases:

- **Small Business (Single Office or Retail Store):** For small companies or retail locations that need a user-friendly, affordable system, **Kisi** is an excellent choice. Its cloud-based management and easy mobile credentials require minimal IT overhead, and pricing is transparent for budgeting. **Brivo** is another strong contender here, offering a proven cloud platform with robust remote management and integration to alarm monitoring (via partners) – ideal if you want a simple system installed and possibly monitored by a service provider. If professional installation plus ongoing support is preferred, **ADT** can design a package that includes not just access control but also intrusion alarms and cameras in one bundle. For very small budgets or DIY inclinations, some might consider ADT's cloud or SimpliSafe's access offering, but those lack the richer features of Kisi or Brivo. Overall, **Kisi** often gets the nod for small businesses due to its ease-of-use, integration with G Suite/Office 365, and modest cost to get started (no servers, low hardware footprint).

- **Mid-Sized Company (Growing SME, Multiple Offices):** Mid-size organizations with dozens of employees and perhaps multiple office sites should look at **Brivo** and **Openpath (Avigilon Alta)** as top options. **Brivo Access** provides a centralized cloud dashboard to manage multiple offices, with features like Apple Wallet credentials and an array of integrations (visitor management, directory services) that suit a growing business. **Avigilon Alta (Openpath)** appeals to tech-oriented firms – its mobile-first, touchless experience will impress employees and its integration with video security (under Motorola) can cover broader security needs. Both allow scaling to new offices easily by just installing more door controllers that connect to the cloud. **Salto KS** is a great fit if the company's offices have many interior doors or unique lock formats (Salto's wireless locks can secure server rooms, cabinets, etc., without wiring) – plus Salto KS's cloud API can integrate with workplace apps for space booking and such. Companies that favor an on-premise approach but still want ease-of-use might opt for **Honeywell WIN-PAK or NetAXS** for a single building (though these will lack some of the cloud convenience) – however, given the trend, a cloud system like Brivo or Openpath usually provides more value and easier multi-site management in this category. For mid-size companies, **Kisi** is also viable, especially if they value quick setup and broad integration (Kisi can scale to dozens of doors across offices with global cloud control, and its pricing remains reasonable as you grow).

- **Enterprise Headquarters or Campus:** Enterprises often require integration with corporate IT, high scalability, and advanced security controls. **Johnson Controls C•CURE 9000** is a top-tier choice for large headquarters or campus environments needing extensive customization – it excels at handling large user counts, complex rule sets, and integration into enterprise ecosystems (like LDAP/AD, video walls, fire systems). Enterprises that have robust IT support and perhaps existing legacy systems might lean to **Honeywell Pro-Watch** or **Lenel (not in top 10 list but another similar enterprise-grade system)**, but among our top 10, Johnson Controls stands out given its ranking and features for enterprise. However, many enterprises are now considering cloud-hybrid models: **Avigilon Alta (Openpath)** under Motorola Solutions could be pitched even at enterprise scale, especially tech companies or those modernizing campuses – it provides enterprise-grade security (SOC2, ISO certified cloud) with a far superior user experience (mobile, cloud) than older systems. In fact, mixing solutions is also a strategy: e.g., use **C•CURE** for core security controlled by security staff, but layer **Openpath** or **Kisi** for flexible office suite management by the IT or workplace team – however, such mixing is complex. If an enterprise values **Mercury open hardware**, they might choose an ACRE solution (Feenics) to keep hardware standard and software cloud-based. Ultimately, enterprises with

dedicated security operations tend to favor **Johnson Controls (Software House)** or **Honeywell** for their proven track record, but forward-leaning enterprises are increasingly adopting **Verkada** or **Openpath** as they renovate offices, because these offer easier scalability across many sites globally and tie-in with other services (Verkada's cameras, for instance, simplify video deployment across an enterprise). For pure office enterprises, **Verkada** can be recommended due to its simple central management and the integrated monitoring – IT departments appreciate not having to maintain servers and the quick user provisioning via SCIM.

- **Co-working Spaces and Flexible Offices:** These environments demand a mix of **scalability, integration with member management, and fluid access sharing**. **Salto KS** has made a name in co-working and flexible office franchises; its API connections with co-work software (like Nexudus, OfficeR&D) automate granting access when a membership is active. Its wireless locks let co-working operators secure private offices and meeting rooms easily, while cloud management handles multi-site operations. **Kisi** is another excellent choice here – Kisi has targeted co-working in its marketing and features (like easy guest link sharing, integration with calendar systems to unlock meeting rooms on schedule) (Source: getkisi.com). In fact, a number of co-working chains have deployed Kisi for its ease of use and the fact that members can use mobile or NFC cards interchangeably. **Openpath (Avigilon Alta)** also suits co-working well: the Wave-to-Unlock and guest pass features create a high-end, seamless experience for members and visitors. The cloud management allows community managers to administer access remotely and in real-time. Brivo could be used too, though Brivo's visitor approach requiring an app might be a slight friction for transient guests – still, Brivo's integration with apps like **Kisi (via Envoy)** or direct would cover visitor registration with QR codes. Given the top 10, **Salto KS** and **Kisi** get top recommendations for co-working due to integration depth and multi-space management focus; **Openpath** is a close third for its slick user experience which can be a selling point for premium co-working brands.

- **Healthcare Facilities (Hospitals, Labs):** Healthcare requires compliance (HIPAA, often JCAHO security standards) and a mix of high-security and flexible access (nurseries vs. public areas). **Honeywell Pro-Watch** or **Johnson Controls** are well-suited for large hospital campuses – they integrate with infant abduction systems, pharmaceutical cabinets, and can implement strict audit trails. They also handle multi-factor authentication at sensitive doors (e.g., requiring a PIN or biometric for medication rooms). However, for smaller clinics or labs, a simpler cloud solution might suffice: **Brivo** or **Kisi** can provide needed security with less infrastructure, and they both support integrations with directory services for managing staff access easily as personnel change. **Dormakaba** shines in healthcare where lots of internal doors exist – its wireless locks can secure patient file rooms, medicine closets etc., without running wires, and Dormakaba has specific solutions for healthcare (they mention industrial and healthcare use). They also offer hospital-grade hardware (anti-bacterial coated locks, etc.). So for a major hospital with unified security command, **Honeywell** or **Johnson (Software House)** is recommended for their comprehensive approach and compliance tools. For a smaller healthcare facility or network of clinics, **Brivo** with its cloud and HIPAA-ready stance (they even mention support for HIPAA compliance) could be a strong choice, providing remote oversight across locations. **Verkada** is also making inroads in healthcare because of its integrated video – security directors appreciate seeing who accessed a pharmacy cabinet immediately via linked camera, for example. But caution in healthcare: ensure whichever system is NDAA compliant (most in top 10 are) and secure from a cybersecurity standpoint (SOC 2, etc., which Kisi, Brivo, Verkada all are).

- **Educational Institutions (Schools & Universities):** Schools prioritize student safety, lockdown capability, and managing many users (students, faculty) on varying schedules. **Salto** is very popular in education (especially higher-ed dormitories and academic buildings) because of its offline/online lock mix – universities can put Salto locks on every dorm room and classroom, using student ID cards as keys, and manage it centrally. The real-time control on perimeter doors with wireless online locks plus the offline capability on interior doors strikes a good balance of cost and security. Many universities have done Salto for residences while maybe using Software House or Lenel for main campus – but Salto can do it all with proper planning. **Dormakaba** also has extensive experience in education (their Keyscan line is used in North American campuses, and their wireless locks for dorms as well). For K-12 schools, ease of use and lockdown function are key: **Kisi** or **Openpath** could be good for a district that wants to centrally manage multiple school buildings with a simple interface and issue mobile credentials to staff (and maybe have fobs for older staff). Kisi even markets hybrid work and local government use cases which parallel school needs (remote management, easy integration with emergency notification) (Source: getkisi.com). That said, K-12 often prefers on-prem for reliability – **Honeywell or JCI** would fit larger districts that integrate access with video and PA systems for emergency response. **Verkada** has specifically targeted K-12 schools as well, with features like lockdown buttons in their interface and immediate camera pop-up on door events, which is valuable in active threat scenarios. Verkada's ease of distribution (cloud-managed across many campuses) and environmental sensors (vape detection in bathrooms) are add-ons that schools like. If a school district values integrated security with minimal IT burden, **Verkada** is a strong recommendation. If a university wants fine control and to leverage existing student IDs, **Salto** or **Dormakaba** gets the recommendation, possibly coupled with an enterprise system for high-security research labs (some labs might even need **Johnson Controls** for government-grade security areas). For cost-conscious schools, **Brivo** or **Kisi** can provide core access control with modest recurring fees and are relatively straightforward, but may need to supplement things like class schedule integration (some SIS integration might be possible through APIs).

In conclusion, the **top 10 solutions each excel in different niches**:

- **Kisi** – best overall for businesses seeking a modern, integration-friendly cloud system; great for SMBs and tech-forward companies.
- **Johnson Controls (C•CURE)** – top for large enterprises/government needing maximal security, integration, and on-prem control.
- **ADT** – ideal for those who want a full-service security package with minimal hassle (e.g., small businesses, retail, franchises) leveraging ADT's monitoring and service network.
- **ACRE/Feenics** – great for enterprises that want cloud software but on open hardware, maintaining flexibility (e.g., those migrating off old Lenel or Software House to cloud).

- **Verkada** – perfect for multi-site organizations and schools that value unified cloud management of access + cameras with an extremely simple user experience and strong security compliance.
- **Brivo** – a tried-and-true cloud pioneer suitable for a wide range of industries (especially multi-property management, commercial real estate, and multi-family residential) where robust integration (e.g., with video, visitor systems) and reliability are important.
- **Avigilon Alta (Openpath)** – an excellent choice for modern offices, multi-tenant buildings, and tech campuses that prioritize sleek hardware design, ease of use, and mobile-first access, now backed by Motorola's ecosystem for expanded capabilities.
- **Dormakaba** – best when a project involves a lot of doors and varied locking needs (hotels, large offices, airports) and you want one vendor for both sophisticated door hardware and the electronic system – it's the go-to for hospitality and often large infrastructure like airports or metros.
- **Salto** – highly recommended for education, co-living/co-working, and any scenario with many dispersed doors and users – it offers a mix of offline and online that can dramatically reduce installation cost while still providing centralized control.
- **Honeywell** – ideal for complex, integrated security environments like hospitals, airports, and industrial campuses that need not just access control but tight linkage with alarms, HVAC, and compliance reporting – Honeywell's longevity and enterprise focus pay off here.

By aligning the organization's needs (cloud vs on-prem, scale, integration, user experience, budget) with the strengths of these solutions, security consultants and facility managers can select a system that not only secures their premises but also enhances operational efficiency and user convenience. The industry is clearly trending towards cloud-managed, mobile-friendly systems, but legacy systems remain relevant for very high-security and customized scenarios. Whichever system is chosen, it's crucial to plan for future scalability, ensure proper training, and engage with certified integrators or the vendor for a successful deployment. With any of these top 10 solutions, when properly implemented, organizations will be well-equipped with a secure, agile, and modern access control infrastructure going forward.

Sources: The above analysis and recommendations reference data and claims from official product documentation and credible industry sources, including Kisi's 2025 access control report, Genea's 2024 comparison blog, 360Connect and Gatewise industry rankings, and vendor security whitepapers (e.g., Brivo, Verkada, Salto), among others, as cited throughout. These citations ensure information is up-to-date and support the evaluation of each solution's features and suitability for various use cases.

Tags: access control systems, physical security, cloud-based management, mobile credentials, security compliance, facility management, system integration

---

About 2727 Coworking

2727 Coworking is a vibrant and thoughtfully designed workspace ideally situated along the picturesque Lachine Canal in Montreal's trendy Griffintown neighborhood. Just steps away from the renowned Atwater Market, members can enjoy scenic canal views and relaxing green-space walks during their breaks.

Accessibility is excellent, boasting an impressive 88 Walk Score, 83 Transit Score, and a perfect 96 Bike Score, making it a "Biker's Paradise". The location is further enhanced by being just 100 meters from the Charlevoix metro station, ensuring a quick, convenient, and weather-proof commute for members and their clients.

The workspace is designed with flexibility and productivity in mind, offering 24/7 secure access—perfect for global teams and night owls. Connectivity is top-tier, with gigabit fibre internet providing fast, low-latency connections ideal for developers, streamers, and virtual meetings. Members can choose from a versatile workspace menu tailored to various budgets, ranging from hot-desks at $300 to dedicated desks at $450 and private offices accommodating 1–10 people priced from $600 to $3,000+. Day passes are competitively priced at $40.

2727 Coworking goes beyond standard offerings by including access to a fully-equipped, 9-seat conference room at no additional charge. Privacy needs are met with dedicated phone booths, while ergonomically designed offices featuring floor-to-ceiling windows, natural wood accents, and abundant greenery foster wellness and productivity.

Amenities abound, including a fully-stocked kitchen with unlimited specialty coffee, tea, and filtered water. Cyclists, runners, and fitness enthusiasts benefit from on-site showers and bike racks, encouraging an eco-conscious commute and active lifestyle. The pet-friendly policy warmly welcomes furry companions, adding to the inclusive and vibrant community atmosphere.

Members enjoy additional perks like outdoor terraces and easy access to canal parks, ideal for mindfulness breaks or casual meetings. Dedicated lockers, mailbox services, comprehensive printing and scanning facilities, and a variety of office supplies and AV gear ensure convenience and efficiency. Safety and security are prioritized through barrier-free access, CCTV surveillance, alarm systems, regular disinfection protocols, and after-hours security.

The workspace boasts exceptional customer satisfaction, reflected in its stellar ratings—5.0/5 on Coworker, 4.9/5 on Google, and 4.7/5 on LiquidSpace—alongside glowing testimonials praising its calm environment, immaculate cleanliness, ergonomic furniture, and attentive staff. The bilingual environment further complements Montreal's cosmopolitan business landscape.

Networking is organically encouraged through an open-concept design, regular community events, and informal networking opportunities in shared spaces and a sun-drenched lounge area facing the canal. Additionally, the building hosts a retail café and provides convenient proximity to gourmet eats at Atwater Market and recreational activities such as kayaking along the stunning canal boardwalk.

Flexible month-to-month terms and transparent online booking streamline scalability for growing startups, with suites available for up to 12 desks to accommodate future expansion effortlessly. Recognized as one of Montreal's top coworking spaces, 2727 Coworking enjoys broad visibility across major platforms including Coworker, LiquidSpace, CoworkingCafe, and Office Hub, underscoring its credibility and popularity in the market.

Overall, 2727 Coworking combines convenience, luxury, productivity, community, and flexibility, creating an ideal workspace tailored to modern professionals and innovative teams.
