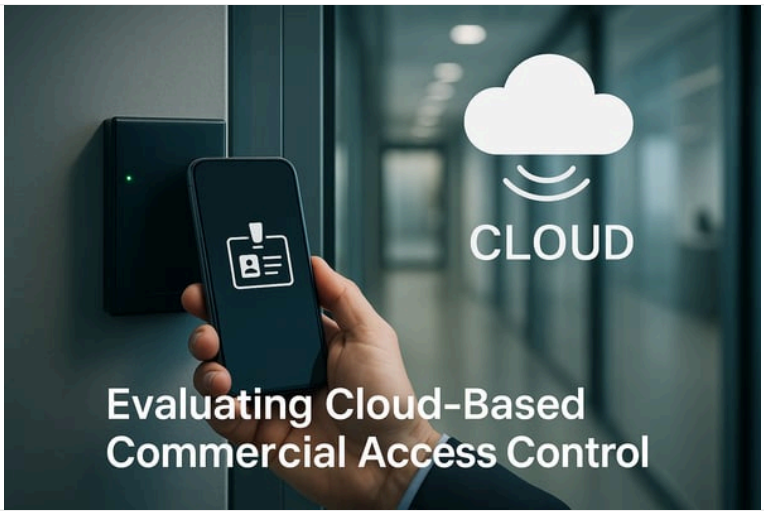
Évaluation des systèmes de contrôle d'accès commerciaux basés sur le cloud

Publié le 30 septembre 2025 95 min de lecture



Top 10 des solutions de contrôle d'accès commercial (2025)

Résumé

Un tableau de bord de contrôle d'accès basé sur le cloud permet la gestion à distance des portes et des utilisateurs.

Les systèmes modernes de contrôle d'accès commercial transforment la manière dont les organisations sécurisent leurs installations. Ce rapport classe les 10 meilleures solutions en 2025, avec **Kisi** en tête de liste comme choix principal. Nous avons évalué chaque système sur des facteurs clés tels que la gestion basée sur le cloud, les identifiants mobiles, les capacités d'intégration, l'évolutivité, la conformité et les fonctionnalités spécifiques à l'industrie. Kisi se distingue par une plateforme cloud intuitive, un accès mobile robuste et des intégrations ouvertes – ce qui lui a valu d'être reconnu comme *« le meilleur système de contrôle d'accès professionnel global »* par un examen indépendant. Parmi les autres principaux concurrents figurent des systèmes d'entreprise établis (Johnson Controls et Honeywell), des plateformes innovantes natives du cloud (Brivo, Openpath/Avigilon Alta, Verkada) et des fournisseurs spécialisés pour les serrures sans fil et les déploiements multi-sites (Salto, Dormakaba, Feenics d'ACRE, etc.). Chaque profil de solution dans ce rapport détaille des ensembles de fonctionnalités tels que la surveillance en temps réel, la gestion des visiteurs, les contrôles de permissions personnalisés, les intégrations tierces (par exemple, les services d'annuaire et les outils de travail), les certifications de sécurité (conformité SOC 2, ISO 27001, GDPR), les modèles de tarification et l'orientation du marché vertical.

En résumé, les meilleurs systèmes de contrôle d'accès combinent la **commodité du cloud**, l'**accès mobile d'abord** et la **sécurité de niveau entreprise**. Les décideurs – des consultants en sécurité aux gestionnaires d'installations – doivent aligner leur choix sur les besoins organisationnels : par exemple, **Kisi** et **Brivo** pour une gestion cloud conviviale à grande échelle, **Johnson Controls** ou **Honeywell** pour les environnements d'entreprise complexes, **Verkada** ou **Openpath (Avigilon Alta)** pour une sécurité unifiée avec intégration vidéo, et **Salto** ou **Dormakaba** pour des solutions matérielles de verrouillage avancées. Les sections suivantes présentent notre méthodologie de classement, la liste complète des 10 meilleurs, des profils de solutions détaillés, une matrice de fonctionnalités et des recommandations adaptées par cas d'utilisation.

Méthodologie de classement

Notre classement est basé sur une analyse complète des capacités de chaque solution, de ses certifications de sécurité, de sa réputation sur le marché et de son applicabilité dans diverses industries. Nous avons recueilli des données à partir de la documentation officielle des produits, des certifications de sécurité, des études de cas clients et des avis fiables de l'industrie (y compris les rapports d'analystes et les blogs sur les technologies de sécurité). Les critères d'évaluation clés comprenaient :

- **Ensemble de fonctionnalités de base :** Disponibilité de tableaux de bord de gestion basés sur le cloud, prise en charge des identifiants mobiles, journaux d'activités et alertes en temps réel, modules de gestion des visiteurs et contrôles de permissions avancés. Par exemple, l'accès mobile/cloud est désormais considéré comme un *« incontournable »* pour les systèmes modernes, de sorte que les solutions dépourvues d'applications mobiles robustes ou de gestion à distance ont obtenu des scores inférieurs.
- **Intégration et écosystème :** Capacité à s'intégrer avec des services tiers tels que les fournisseurs d'identité (Google Workspace, Microsoft Azure AD/Entra ID, Okta), les outils de communication, les systèmes de vidéosurveillance et les plateformes de gestion de bâtiments. La disponibilité d'API ouvertes et la prise en charge de matériel standard (contrôleurs Mercury, lecteurs à protocole ouvert) étaient des points positifs. Les systèmes avec du matériel propriétaire ou des logiciels cloisonnés ont été notés.
- **Évolutivité et fiabilité :** Performance dans les déploiements multi-sites ou d'entreprise, fiabilité hors ligne (fonctionnement continu pendant les pannes de réseau) et nombre élevé d'utilisateurs/portes. Nous avons pris en compte toute limite d'expansion (par exemple, les plafonds de lecteurs ou d'événements) et si l'architecture est véritablement évolutive dans le cloud ou un système sur site équipé de connecteurs cloud.
- **Sécurité et conformité :** Certifications telles que SOC 2 Type II et ISO 27001, conformité au GDPR et autres lois sur la protection des données, et adhésion aux normes de sécurité de l'industrie (chiffrement, matériel conforme NDAA, FIPS, etc.). Les certifications vérifiées (SOC 2, ISO 27001) ont été fortement pondérées pour garantir la fiabilité du fournisseur.
- **Transparence des prix et TCO :** Clarté des modèles de tarification (prix publiés vs. devis personnalisés), frais de licence pour des fonctionnalités telles que les identifiants mobiles, et rentabilité globale. Les solutions avec des prix clairs et publiés (par exemple, Kisi) ont obtenu des points pour la transparence, tandis que les fournisseurs historiques nécessitant des devis personnalisés ont été évalués qualitativement.
- **Adoption et personnalisation par l'industrie :** Preuve de succès dans des secteurs verticaux spécifiques (par exemple, espaces de coworking, bureaux d'entreprise, santé, éducation, résidentiel multifamilial). Nous avons recherché des fonctionnalités adaptées aux besoins de l'industrie – par exemple, des intégrations avec des systèmes de gestion immobilière dans le résidentiel multifamilial, ou la conformité aux réglementations de sécurité gouvernementales et de la santé pour les entreprises. Les catégories « idéal pour » de chaque solution ont été prises en compte (par exemple, Kisi est noté pour les PME et les bureaux, Honeywell pour les grandes installations comme les aéroports).

Chaque système a été étudié avec des informations à jour à la mi-2025. Notre méthodologie a assuré une comparaison impartiale, fonctionnalité par fonctionnalité, afin de fournir aux professionnels une compréhension claire du paysage.

Tableau de classement complet des 10 meilleures solutions

Vous trouverez ci-dessous un aperçu des 10 meilleures solutions de contrôle d'accès commercial pour 2025, classées par ordre. Ce tableau répertorie chaque solution, son type général de solution et un point fort clé ou un cas d'utilisation idéal :

CLASSEMENT	SOLUTION	TYPE DE SOLUTION ET CAS D'UTILISATION IDÉAL
1.	**Kisi**	Plateforme d'accès basée sur le cloud et axée sur le mobile – la meilleure solution globale pour les bureaux modernes et les PME, avec de nombreuses intégrations.
2.	**Johnson Controls (C•CURE)**	Solution d'entreprise sur site et hybride cloud – idéale pour les grandes entreprises et les installations de haute sécurité nécessitant une intégration étendue (vidéo, incendie, intrusion).
3.	**ADT**	Solution de sécurité complète – personnalisable pour toutes les tailles, avec surveillance 24h/24 et 7j/7 et intégration de l'accès, de la vidéo et des alarmes (populaire pour le commerce de détail, les franchises, etc.).
4.	**ACRE (Feenics/Vanderbilt)**	Systèmes basés sur Mercury et compatibles cloud – flexibles pour les entreprises qui préfèrent le matériel non propriétaire et ont besoin de fonctionnalités telles que le confinement d'urgence et les bornes visiteurs.
5.	**Verkada**	Plateforme de sécurité hybride cloud – idéale pour les organisations axées sur l'informatique recherchant un accès unifié + vidéo sur une interface cloud simple, évolutive de dix à des milliers de portes.
6.	**Brivo**	Contrôle d'accès cloud pionnier – excellent pour les entreprises multi-sites et le résidentiel multifamilial, offrant des intégrations API robustes et une gestion conviviale via web/mobile.
7.	**Avigilon Alta (Openpath)**	Accès cloud mobile-centrique (Motorola Solutions) – adapté aux espaces de travail modernes et aux communautés multifamiliales, avec entrée sans contact par smartphone et forte intégration d'interphones vidéo.
8.	**Dormakaba**	Solution matérielle-logicielle intégrée – leader mondial des serrures et systèmes d'entrée, idéale pour les entreprises ayant besoin de serrures électroniques transparentes (portes, tourniquets, etc.) et d'intégrations hôtelières.
9.	**Salto**	Plateforme de serrures intelligentes sans fil – idéale pour les environnements de campus (éducation, hôtellerie) nécessitant des solutions d'entrée sans clé flexibles et une évolutivité facile avec la gestion cloud.
10.	**Honeywell**	Suite de sécurité d'entreprise – éprouvée pour les grands campus et les infrastructures critiques (aéroports, hôpitaux) avec un contrôle d'accès complet lié à l'incendie, au CVC et à l'automatisation des bâtiments.

Note du tableau : Avigilon Alta est le produit d'accès cloud Openpath renommé sous Motorola Solutions. Le portefeuille d'ACRE comprend Feenics (Keep) pour l'accès cloud et Vanderbilt Industries pour les systèmes sur site. Johnson Controls inclut les gammes Tyco Software House (C•CURE 9000) et Kantech. Le profil détaillé de chaque solution est fourni dans la section suivante.

Profils détaillés de chaque solution (1 à 10)

1. Kisi

Présentation : Kisi est un fournisseur de contrôle d'accès basé sur le cloud, réputé pour son logiciel facile à utiliser et son accès mobile fluide. En tant que véritable solution cloud, Kisi permet aux administrateurs de gérer les portes et les identifiants depuis n'importe où via un tableau de bord web ou une application mobile. Il combine du **matériel intelligent** (contrôleurs et lecteurs professionnels propriétaires Kisi) avec une plateforme ouverte qui s'intègre aux systèmes informatiques et de sécurité existants. Les entreprises technophiles apprécient l'interface conviviale de Kisi et l'élimination des serveurs sur site.

Fonctionnalités clés :

- **Gestion cloud :** Tableau de bord cloud centralisé pour la surveillance en temps réel, les déverrouillages à distance et les journaux d'audit. Les administrateurs peuvent ajuster instantanément les permissions ou consulter les événements de porte depuis n'importe quel endroit. Le système est continuellement mis à jour avec de nouvelles fonctionnalités via le cloud.
- **Accès mobile et sans clé :** Application mobile robuste (iOS/Android) qui transforme les smartphones en clés, prenant en charge le Bluetooth, le NFC et même les badges *Apple Wallet* pour l'entrée. Cela offre une expérience d'entrée fluide et sans contact. Les cartes/porte-clés traditionnels (chiffrés AES 128 bits) sont également pris en charge pour une utilisation hybride.
- **Intégration et API :** API ouverte et des dizaines d'intégrations prêtes à l'emploi. Kisi peut se synchroniser avec les **services d'annuaire** (Azure AD, Okta, Google Workspace) pour automatiser l'intégration/la désintégration des employés, avec les **outils de communication** comme Slack pour les notifications d'entrée, et avec les plateformes de **gestion des visiteurs** (par exemple, Envoy) pour simplifier l'accès des invités. Il s'intègre également aux appareils IoT (serrures sans fil d'Allegion, caméras de sécurité, panneaux d'alarme) pour créer un système unifié.
- **Évolutivité :** Convient pour une seule porte jusqu'aux déploiements multi-bureaux d'entreprise. L'architecture cloud de Kisi et l'approche *One Security Platform* s'adaptent à l'échelle mondiale tout en maintenant un contrôle centralisé (Source: getkisi.com. (Remarque : Les très grands déploiements peuvent nécessiter plusieurs contrôleurs – chaque contrôleur Kisi prend en charge 4 portes – ce qui est une considération pour les sites avec des centaines de portes.)
- **Gestion des visiteurs :** Offre un module intégré d'**accès visiteurs** qui délivre des laissez-passer temporaires par code QR ou des identifiants basés sur des liens aux invités pour une entrée sans application. Cela modernise l'enregistrement des visiteurs et fonctionne de manière transparente avec les portes contrôlées par Kisi.
- **Surveillance en temps réel :** Fournit des événements de porte en direct, des alertes personnalisables (par exemple, porte laissée ouverte, entrée forcée) et des analyses de rapports. Les administrateurs peuvent recevoir des notifications instantanées pour les événements critiques et examiner les pistes d'audit par utilisateur ou par porte.
- **Permissions personnalisées :** Règles d'accès granulaires par groupes d'utilisateurs, horaires et rôles. Kisi prend en charge l'accès basé sur le temps (par exemple, uniquement pendant les heures de bureau ou des quarts de travail spécifiques) et les restrictions basées sur l'emplacement sur plusieurs sites. Les bureaux mondiaux peuvent être gérés sous un seul système avec une segmentation locale des permissions.
- **Déverrouillage et administration à distance :** Les portes peuvent être déverrouillées ou verrouillées à distance via l'application ou le web Kisi, prenant en charge des cas d'utilisation tels que l'accès du personnel de livraison en dehors des heures de bureau ou le déclenchement d'un confinement d'urgence dans une installation.
- **Sécurité et conformité :** Kisi est certifié indépendamment **ISO 27001** et **SOC 2 Type II**, soulignant de solides pratiques de sécurité des données. Il est conforme aux exigences GDPR, CCPA et NDAA. Les données sont chiffrées en transit et au repos, et des tests d'intrusion réguliers sont effectués pour garantir la résilience du système.

- **Tarification :** Kisi est l'un des rares acteurs de ce secteur à proposer une tarification transparente. Le matériel (contrôleurs et lecteurs) est vendu à l'avance (environ 599 à 699 $ par lecteur et 899 $ par contrôleur) et le logiciel cloud est basé sur un abonnement d'environ 49 $ par porte par mois. Il n'y a pas de frais par utilisateur, et les identifiants mobiles sont illimités avec le service – offrant un modèle rentable par rapport aux systèmes hérités qui facturent par identifiant.
- **Cas d'utilisation par industrie :** Les petites et moyennes entreprises sont un marché de prédilection pour Kisi, y compris les espaces de coworking, les bureaux modernes, les studios de fitness et les établissements d'enseignement. Les entreprises ayant une stratégie informatique « cloud-first » adoptent également Kisi pour sa flexibilité. Sa capacité à s'intégrer avec des logiciels spécifiques à l'industrie (par exemple, Optix pour le coworking, les systèmes de gestion de club pour les salles de sport) le rend adaptable. Les clients d'entreprise utilisent Kisi pour gérer des bureaux mondiaux avec des politiques unifiées.

Points forts notables : La facilité d'installation et de configuration de Kisi est fréquemment saluée – il peut être installé sur n'importe quelle gâche électrique ou serrure magnétique avec un câblage minimal, souvent en quelques minutes. Son approche mobile-centrique et son *application unifiée* (employés, administrateurs et même invités utilisent tous une seule application ou un système basé sur des liens) se distinguent, surtout par rapport à certains concurrents qui nécessitent plusieurs applications pour différentes fonctions. Les intégrations (plus de 20 et en croissance) permettent à Kisi de s'adapter à n'importe quelle pile technologique, automatisant des flux de travail comme la révocation d'accès lorsqu'un système RH marque un employé comme licencié. De plus, l'**engagement de Kisi en matière de sécurité** (SOC 2, ISO 27001) est comparable à celui des leaders de l'industrie, ce qui est rassurant pour les équipes informatiques et de sécurité.

Inconvénients potentiels : En tant que système propriétaire, Kisi nécessite l'utilisation de ses contrôleurs et lecteurs (bien qu'ils fonctionnent avec le matériel de porte standard). Cette approche de « matériel fermé » signifie que les panneaux tiers existants doivent généralement être remplacés lors du passage à Kisi. Cependant, l'API ouverte de Kisi atténue le verrouillage propriétaire côté logiciel en s'intégrant à d'autres systèmes. Pour les très grandes installations (des centaines de portes), l'installation de nombreux contrôleurs Kisi pourrait être une considération logistique, bien que le logiciel cloud s'adapte sans problème. Enfin, bien que Kisi propose désormais la gestion des visiteurs, elle est relativement basique (principalement des liens par code QR/e-mail) et moins riche en fonctionnalités que certains systèmes de visiteurs dédiés – les organisations ayant des flux de travail de visiteurs importants pourraient intégrer une solution partenaire pour des capacités supplémentaires.

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

Présentation : Johnson Controls (JCI) propose certains des systèmes de contrôle d'accès les plus établis sur le marché, principalement la plateforme **Software House C•CURE 9000** et les systèmes **Kantech** (suite à la fusion de JCI avec Tyco). Ces solutions sont des piliers de l'industrie depuis des décennies dans les grandes entreprises, les gouvernements et les environnements de haute sécurité. Le portefeuille de JCI évolue pour inclure des options gérées dans le cloud comme *C•CURE 9000 Cloud* et *Tyco Cloud*, mais leurs offres principales restent des systèmes sur site robustes avec hébergement cloud optionnel. Les systèmes JCI sont reconnus pour leur **évolutivité** (gérant des milliers de portes et de titulaires de cartes), leur intégration profonde avec les systèmes de sécurité des bâtiments et leur conformité aux normes gouvernementales strictes.

Fonctionnalités clés :

- **Déploiements cloud ou sur site :** Traditionnellement déployé sous forme de serveurs sur site avec un logiciel client lourd pour le contrôle, C•CURE 9000 peut désormais être hébergé dans le cloud ou fonctionner en mode hybride. Johnson Controls a introduit **C•CURE Cloud** (hébergé sur AWS) qui maintient une parité fonctionnelle complète tout en réduisant l'empreinte informatique sur site. Ce service cloud est construit sur une infrastructure conforme SOC 2 et prend même en charge les normes gouvernementales FICAM pour les déploiements fédéraux. Pour les installations plus petites, la gamme **Kantech** de JCI (par exemple, le logiciel EntraPass) offre une gestion web plus simple ou des options hébergées.
- **Évolutivité d'entreprise :** Capable de gérer *des dizaines de milliers d'utilisateurs et d'événements par jour* sur plusieurs installations. L'architecture prend en charge le traitement distribué – par exemple, **C•CURE 9000** peut utiliser des serveurs d'applications en cluster et les **contrôleurs iSTAR** gèrent les décisions locales en cas de perte de réseau. JCI revendique une capacité de porte pratiquement illimitée dans son édition entreprise, ce qui la rend adaptée aux très grands campus et aux entreprises mondiales.
- **Intégration matérielle :** Les systèmes de JCI utilisent du **matériel ouvert** dans de nombreux cas – par exemple, les contrôleurs Kantech et les nouveaux appareils iSTAR Edge sont compatibles Mercury ou de standard ouvert, permettant une certaine flexibilité. Cependant, C•CURE utilise traditionnellement des panneaux iSTAR propriétaires. Les solutions JCI s'intègrent étroitement aux **lecteurs HID** (y compris les lecteurs biométriques) et prennent en charge les identifiants multi-technologies (Prox, iCLASS, DESFire, etc.). Le portefeuille matériel est vaste : des contrôleurs de porte IP aux lecteurs de cartes à puce chiffrés et aux intégrations de serrures sans fil.
- **Logiciel et analyses :** La suite logicielle C•CURE est riche en fonctionnalités : surveillance des alarmes en temps réel, gestion des niveaux de menace (par exemple, modes de confinement par simple pression d'un bouton), rapports de rassemblement pour les urgences, et un moteur de règles pour programmer des flux de travail de sécurité complexes. Elle comprend un module de gestion des identités et peut s'intégrer aux bases de données RH pour le provisionnement. L'interface utilisateur est complexe mais hautement personnalisable – les opérateurs de sécurité peuvent afficher des plans d'étage interactifs avec l'état des portes, et configurer des réponses basées sur des flux de travail aux incidents. JCI propose également des **rapports et des analyses** pour la conformité (par exemple, les fonctionnalités PIAM – gestion des identités physiques et des accès).
- **Gestion des visiteurs :** Un module de *gestion des visiteurs natif* est disponible (par exemple, *C•CURE 9000 Visitor Management*), permettant la pré-inscription des invités, l'impression de badges, les notifications aux hôtes, etc. C'est bénéfique pour les entreprises qui souhaitent une solution tout-en-un. Cependant, il peut ne pas être aussi moderne que les applications de visiteurs spécialisées ; de nombreux clients JCI intègrent également des systèmes de visiteurs tiers.
- **Accès mobile et à distance :** Historiquement une faiblesse – les anciens systèmes JCI étaient conçus pour un contrôle basé sur PC. Cependant, JCI a lancé l'**application sécurisée Honeywell/Johnson Controls** (pour sa gamme de produits de sécurité) qui offre une surveillance mobile et un contrôle de porte de base (Source: play.google.com. En pratique, de nombreux déploiements JCI utilisent *HID Mobile Access* pour les identifiants mobiles (étant donné que le matériel HID Global est souvent utilisé) – ce qui signifie que les employés peuvent taper leur téléphone via BLE/NFC sur les lecteurs HID pour entrer. Le *support Apple Wallet* pour les badges d'employés n'est pas mentionné nativement, mais en utilisant la plateforme de HID, cela peut être réalisé. L'administration mobile complète (ajout d'utilisateurs, déverrouillages à distance via l'application) est encore en cours de développement mais s'améliore via les nouvelles interfaces web et applications.
- **Intégrations tierces :** Les solutions Johnson Controls excellent dans les intégrations pour la **vidéosurveillance, les alarmes et les systèmes de bâtiment**. C•CURE, par exemple, s'intègre aux **systèmes de gestion vidéo** (comme American Dynamics victor, ExacqVision, Milestone) pour lier les événements de porte à la vidéo. Il s'intègre également aux panneaux de **détection d'intrusion** et aux systèmes d'interphone pour une gestion unifiée des alarmes. Pour l'intégration informatique, JCI prend en charge la synchronisation Active Directory pour les données utilisateur, et le canal sécurisé OSDP pour les communications des lecteurs. Il existe également des SDK et des API pour les intégrations personnalisées. Certaines intégrations cloud (comme le provisionnement SCIM ou la synchronisation des utilisateurs Azure AD) peuvent ne pas être aussi plug-and-play que dans les nouvelles solutions natives du cloud, mais peuvent être réalisées avec des services professionnels.
- **Conformité et sécurité :** Le contrôle d'accès de JCI est fiable dans les environnements de haute sécurité – il offre un chiffrement de bout en bout (AES 256) entre les contrôleurs et le logiciel, et des options pour les composants validés **FIPS 140-2** pour une utilisation gouvernementale. Les offres hébergées dans le cloud sont construites sur des plateformes sécurisées (OpenShift sur AWS) avec conformité SOC 2. JCI est également conforme aux normes spécifiques de l'industrie (par exemple, leur support PIV pour les identifiants gouvernementaux via FIPS 201). L'entreprise met l'accent sur les pratiques de cybersécurité et dispose d'une équipe dédiée à la sécurité des produits ; leurs systèmes subissent des modélisations de menaces et des mises à jour régulières (le programme **Johnson Controls Security Lifecycle**).
- **Tarification :** Les solutions Johnson Controls sont vendues par l'intermédiaire de partenaires intégrateurs et la tarification est **basée sur devis**. Généralement, il y a des frais de licence par porte ou par lecteur pour le logiciel, plus des contrats de maintenance logicielle annuels. Les systèmes d'entreprise comme C•CURE ont un coût initial plus élevé et des frais de support continus. Le nouveau modèle d'abonnement cloud (Tyco Cloud) passe probablement à des frais SaaS récurrents. *La transparence des prix est faible* – les clients doivent contacter un revendeur certifié pour obtenir des devis. À titre de référence, le coût total par porte (incluant le matériel, la licence logicielle et l'installation) peut être élevé (souvent 1500 à 3000 $ par porte dans les scénarios d'entreprise), mais il offre des fonctionnalités robustes.

Points forts notables : Johnson Controls (via les marques de Tyco) a fait ses preuves dans les déploiements à grande échelle – de nombreuses entreprises du Fortune 500, des agences gouvernementales et des sites d'infrastructure critique s'appuient sur C•CURE ou Kantech. Les systèmes sont extrêmement **riches en fonctionnalités et personnalisables**, prenant en charge des politiques de sécurité complexes (par exemple, double authentification à certaines portes, règles anti-passback, scénarios de confinement, etc.). L'étendue de l'intégration est un atout majeur : on peut gérer la vidéo, l'accès et les alarmes dans une seule interface pour une gestion holistique de la sécurité. La capacité à mélanger et assortir les composants hébergés et sur site offre une flexibilité ; par exemple, un client pourrait avoir un serveur sur site au siège social et utiliser un portail cloud pour les sites régionaux. De plus, la **scalabilité et la fiabilité** sont de premier ordre – ces systèmes ont rarement des limites strictes qu'une entreprise normale atteindrait, et ils prennent en charge la redondance et le basculement pour une haute disponibilité.

Inconvénients potentiels : La contrepartie de la puissance et de l'échelle est la complexité. Les interfaces de JCI (C•CURE en particulier) peuvent être **moins conviviales** et nécessitent des techniciens certifiés pour la configuration et les modifications. La gestion quotidienne peut exiger plus de formation par rapport à la simplicité des nouvelles solutions cloud. Pour les petites organisations sans personnel informatique de sécurité dédié, les systèmes JCI peuvent être excessifs. De plus, le **coût est significatif** – non seulement le coût initial, mais aussi la maintenance continue et le besoin de support professionnel. La dépendance à des éléments propriétaires (dans certains cas) peut créer un verrouillage fournisseur, bien que JCI se soit orienté vers l'ouverture avec le matériel Mercury. Un autre inconvénient a été l'adoption lente de certaines commodités modernes – par exemple, *aucune intégration native Apple/Google Wallet* prête à l'emploi (contrairement à Kisi ou Brivo), et jusqu'à récemment aucune application mobile unifiée pour les administrateurs. Cependant, JCI s'attaque à certains de ces problèmes avec son portail cloud et ses offres mobiles en évolution. Enfin, parce que les systèmes JCI sont généralement installés par des intégrateurs tiers, l'**expérience client** peut varier – la réactivité du support dépend du revendeur local, ce qui peut être un point sensible par rapport aux modèles de support direct de certains fournisseurs cloud.

3. Contrôle d'accès ADT

Présentation : ADT est un nom bien connu dans le domaine de la sécurité, et sa division commerciale propose un contrôle d'accès intégré dans le cadre d'offres de sécurité plus larges. Plutôt qu'une plateforme propriétaire unique, **ADT agit comme un fournisseur/intégrateur de solutions**, livrant souvent un système personnalisé utilisant du matériel/logiciel de divers fabricants (y compris leurs propres solutions et partenaires de marque). La proposition de valeur d'ADT est un **guichet unique** : ils conçoivent, installent, surveillent et entretiennent l'ensemble du système de sécurité – y compris le contrôle d'accès, les alarmes d'intrusion et la vidéosurveillance – en particulier pour les petites et moyennes entreprises. La longue histoire d'ADT (depuis 1874) dans la télésurveillance lui confère une solide base de services pour un support 24h/24 et 7j/7.

Fonctionnalités clés :

- **Solutions personnalisables :** ADT n'impose pas une plateforme unique – ils adaptent le système aux besoins du client. Par exemple, une solution pourrait utiliser des **contrôleurs Honeywell ou Lenel** pour une installation plus grande, ou **Brivo/Alarm.com Cloud** pour les plus petites. La propre plateforme de contrôle d'accès d'ADT (anciennement ADT Select ou ADT Enterprise) utilise souvent des panneaux basés sur Mercury avec l'enveloppe logicielle d'ADT. Cette flexibilité signifie qu'un système ADT peut être aussi simple ou avancé que nécessaire, d'un système de carte d'accès à une seule porte à un déploiement d'entreprise multi-sites. La configuration est *entièrement personnalisable* pour répondre aux exigences et au budget.
- **Fonctionnalités de sécurité intégrées :** Une caractéristique distinctive de l'offre d'ADT est l'intégration du **contrôle d'accès avec la vidéosurveillance et la détection d'intrusion**. Par exemple, un système d'accès ADT peut lier les portes aux caméras ADT de sorte que lorsqu'une porte est ouverte, un enregistrement est déclenché. De même, il peut se connecter aux systèmes d'alarme – par exemple, utiliser un événement de porte forcée pour déclencher une alarme ou notifier l'état du panneau d'intrusion sur la même application. De nombreux concurrents proposent des intégrations, mais l'avantage d'ADT est qu'ils le livrent sous forme de package unifié (et souvent avec une seule interface pour l'utilisateur final, comme les applications Pulse ou Control d'ADT pour les PME).
- **Gestion à distance :** ADT fournit des outils de **surveillance et de gestion à distance** afin que les clients puissent contrôler leur système hors site. L'application mobile professionnelle d'ADT (souvent ADT Control for Business) permet aux propriétaires de verrouiller/déverrouiller les portes, de recevoir des alertes et même de gérer les codes ou cartes d'utilisateur à distance. Les petites entreprises, par exemple, peuvent armer/désarmer les alarmes et déverrouiller les portes depuis un téléphone. ADT souligne que *l'ensemble du système peut être contrôlé à distance*, reflétant la poussée vers la connectivité cloud.
- **Méthodes d'accès :** Les installations ADT typiques prennent en charge les **cartes d'accès, les porte-clés, les codes PIN et les identifiants mobiles**. ADT annonce la possibilité d'utiliser les téléphones mobiles comme identifiants d'accès (probablement en utilisant les identifiants mobiles HID ou la plateforme d'identifiants mobiles d'Alarm.com). Des lecteurs biométriques ou des interphones peuvent également être incorporés si nécessaire. Ils proposent également des **postes d'interphone bidirectionnels** aux points d'entrée, permettant au personnel de sécurité ou au personnel de communiquer avec les visiteurs avant d'accorder l'accès – utile pour les entrées clôturées ou les portes de hall.
- **Gestion des visiteurs et des entrepreneurs :** Bien qu'ADT n'ait pas d'application propriétaire de gestion des visiteurs, ils configurent souvent des systèmes pour faciliter l'entrée des visiteurs via interphone ou clavier. Ils peuvent intégrer des systèmes comme **Envoy ou Traction Guest** sur demande. Pour les entrepreneurs ou les livraisons, les solutions d'ADT incluent souvent des codes d'accès programmés ou un déverrouillage à distance via l'application du propriétaire de l'entreprise. L'accent est mis sur la commodité pour les propriétaires d'entreprise d'autoriser les visiteurs sans avoir à être sur place.
- **Services de surveillance :** Un aspect unique est l'option de **surveillance professionnelle 24h/24 et 7j/7** d'ADT. Par exemple, si le système d'accès est lié à une alarme et qu'une entrée forcée se produit après les heures de bureau, le centre de surveillance d'ADT interviendra et dépêchera les autorités si nécessaire. Cette couche de service distingue ADT des systèmes purement DIY ou non surveillés. Elle externalise essentiellement une partie de la gestion de la sécurité à l'équipe d'ADT moyennant des frais supplémentaires, ce que de nombreuses entreprises trouvent précieux.
- **Scalabilité :** ADT dessert toutes les échelles, mais est particulièrement populaire auprès des **petites et moyennes entreprises et des chaînes de magasins**. Ils soulignent que le système peut *s'adapter à la hausse ou à la baisse en fonction de l'évolution des besoins de l'entreprise*. Par exemple, l'ajout de nouvelles portes ou de nouveaux emplacements peut être effectué facilement sous l'égide d'ADT. Cela dit, les très grandes entreprises ayant des besoins complexes pourraient opter pour des systèmes spécialisés (qu'ADT pourrait toujours mettre en œuvre en tant qu'installateur). ADT Commercial (une division distincte) gère des projets plus importants en utilisant des plateformes de niveau entreprise (ils pourraient déployer LenelS2 ou S2 NetBox pour un campus d'entreprise sous leur gestion).
- **Sécurité et conformité :** ADT s'appuie sur la sécurité du système sous-jacent qu'ils installent. Ils garantissent que les signaux et les données sont cryptés (en particulier les signaux d'alarme vers leurs centres de surveillance). ADT est certifié UL pour les installations d'alarme et s'assure probablement que tous les composants cloud sont sur une infrastructure sécurisée. Cependant, ADT ne met pas publiquement en avant SOC 2 ou ISO 27001 comme le font les fournisseurs de logiciels purs, car ils sont davantage un intégrateur. Pour la conformité (comme le GDPR ou la confidentialité), ils se réfèrent aux plateformes utilisées (de nombreux systèmes cloud fournis par ADT sont basés sur Alarm.com qui dispose d'une sécurité cloud robuste).
- **Tarification :** Le modèle d'ADT implique généralement des coûts d'installation initiaux plus un abonnement récurrent pour la surveillance et l'accès au cloud. La **tarification n'est pas transparente** publiquement ; elle est fournie via des consultations de devis gratuites. Cependant, ADT propose souvent des promotions. Pour une petite entreprise, on pourrait payer quelques centaines de dollars pour l'équipement/l'installation par porte, puis des frais mensuels (qui pourraient être de l'ordre de 40 à 100 $/mois pour un forfait alarme + accès + vidéosurveillance). Le devis est personnalisé pour inclure tous les composants nécessaires. La force d'ADT est d'offrir le *financement ou la location* d'équipement en échange de contrats de service pluriannuels, ce qui en fait une dépense d'exploitation prévisible pour les entreprises.

Points forts notables : La principale force d'ADT est la **simplicité et le support**. Les propriétaires d'entreprise qui n'ont pas de personnel de sécurité ou informatique dédié peuvent compter sur ADT pour gérer la conception, l'installation et la gestion continue du système. Les solutions d'ADT sont **installées professionnellement** et incluent une formation, ce qui élimine beaucoup de tracas. L'intégration de la télésurveillance d'alarme d'intrusion avec le contrôle d'accès est également un grand avantage – un seul fournisseur couvre les deux, il n'y a donc pas de renvoi de responsabilité entre des entreprises d'alarme et d'accès distinctes. Le service de télésurveillance centralisé de longue date d'ADT est un différenciateur ; peu d'autres sur cette liste offrent une surveillance en direct des événements d'accès. Pour les commerces de détail ou les franchises multi-sites, ADT peut fournir une solution cohérente sur tous les sites et un point de contact unique pour le support. De plus, les systèmes d'ADT sont assez **complets en fonctionnalités pour les besoins des PME** : gestion à distance, analyses de base (comme les rapports d'accès, les données de temps et de présence), et la tranquillité d'esprit d'une marque fiable.

Inconvénients potentiels : Comme ADT utilise diverses technologies sous-jacentes, l'**ensemble des fonctionnalités peut varier**. Vous dépendez quelque peu du choix de plateforme d'ADT, qui pourrait ne pas être aussi avant-gardiste que certains concurrents spécialisés. Par exemple, ADT pourrait ne pas offrir immédiatement des fonctionnalités comme les badges d'employés Apple Wallet ou les codes QR avancés pour les visiteurs, à moins que la plateforme choisie ne les prenne en charge. Il y a aussi généralement **moins de transparence** dans la technologie – l'utilisateur interagit principalement avec le portail ou l'application d'ADT, ce qui pourrait masquer un système tiers. Si un client souhaitait une autogestion à un niveau profond (par exemple, intégrer un nouveau logiciel via API), cela pourrait être difficile avec ADT à moins qu'ils ne le facilitent. Un autre inconvénient peut être le **coût à long terme** – la commodité et le service d'ADT ont un prix. Les contrats à long terme avec renouvellements automatiques sont courants, et l'annulation anticipée peut entraîner des frais. Certains clients signalent que les éléments propriétaires ou les termes du contrat rendent coûteux le passage à un autre fournisseur qu'ADT. Enfin, l'accent mis par ADT sur le service signifie que l'**expérience utilisateur pourrait être moins configurable** par le client – par exemple, des règles personnalisées avancées ou des intégrations nécessiteraient de contacter le support ADT plutôt que de le faire soi-même. Pour les clients très axés sur la technologie qui préfèrent un contrôle direct et une personnalisation, cela peut être limitant. Dans l'ensemble, ADT est idéal pour ceux qui veulent que la sécurité soit gérée pour eux, mais moins pour ceux qui veulent bricoler ou ont des besoins d'intégration technologique uniques et évolutifs.

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

Présentation : ACRE est une société mère qui a regroupé plusieurs marques de contrôle d'accès, notamment **Feenics (Keep)**, **Vanderbilt Industries (ACT)**, **RS2 Technologies** et **Open Options**. Grâce à ces marques, ACRE offre un portefeuille complet allant du contrôle d'accès purement cloud aux systèmes d'entreprise sur site. Dans notre contexte, nous nous concentrons sur la plateforme cloud phare d'ACRE, *Feenics Keep*, et les offres connexes. Les solutions d'ACRE sont connues pour utiliser largement le **matériel non propriétaire Mercury**, offrant aux clients la flexibilité d'éviter le verrouillage fournisseur. Elles sont riches en fonctionnalités et basées sur des standards, attirant les entreprises et les intégrateurs qui valorisent l'ouverture.

Fonctionnalités clés :

- **Plateforme basée sur le cloud (Feenics) :** Feenics (acquise par ACRE en 2021) propose *Keep by Feenics*, une véritable solution de contrôle d'accès cloud hébergée sur Amazon Web Services. Keep est conçue comme une plateforme SaaS multi-locataires, ce qui signifie que les intégrateurs ou les clients finaux peuvent gérer le contrôle d'accès via un navigateur web sans serveurs locaux. Elle prend en charge toutes les fonctions essentielles (ajouter des utilisateurs, attribuer des identifiants, définir des horaires, surveiller les événements) via une interface intuitive. Une fonctionnalité notable est une capacité intégrée de **« Confinement d'urgence »** qui peut sécuriser toutes les portes instantanément via le cloud en cas de crise. De plus, Feenics prend en charge les **notifications de masse**, afin que les administrateurs de sécurité puissent envoyer des alertes aux employés pendant les urgences.
- **Matériel ouvert (Mercury Powered) :** Les systèmes d'ACRE (Feenics, RS2, Open Options, et même les systèmes d'entreprise de Vanderbilt) sont largement construits sur des contrôleurs **Mercury Security**. Mercury est une plateforme matérielle standard de l'industrie utilisée par de nombreux fournisseurs, ce qui signifie que les solutions ACRE peuvent souvent fonctionner avec des cartes Mercury existantes ou du moins être migrées vers/depuis d'autres systèmes basés sur Mercury avec un échange de matériel minimal. Cette approche non propriétaire donne aux clients la liberté de changer de logiciel à l'avenir sans avoir à remplacer tous les contrôleurs. Elle assure également la compatibilité avec une large gamme de matériel de lecture (HID, Allegion Schlage, NXP, etc.).
- **Capacités d'intégration :** Feenics Keep offre une **API RESTful ouverte** et une liste croissante d'intégrations (environ 20+ intégrations pré-construites en 2024). Celles-ci incluent la liaison avec des **systèmes RH** comme Workday pour la provisionnement automatique de l'accès lorsqu'un nouvel employé est ajouté, et avec des **kiosques de gestion des visiteurs** (Feenics dispose d'un module natif de gestion des visiteurs et d'une application de kiosque basée sur tablette). Il peut s'intégrer à la gestion des identités (via Okta ou Azure AD en utilisant SCIM), et à des plateformes vidéo tierces – bien que l'analyse de Genea ait noté que Feenics avait *moins d'intégrations de gestion vidéo* prêtes à l'emploi par rapport à certains concurrents. Manquaient notamment des intégrations directes avec Cisco Meraki Video, Rhombus ou Eagle Eye au moment de cette analyse. Cependant, les sorties d'alarme de base peuvent déclencher des systèmes externes et vice versa. L'intégration du contrôle d'ascenseur est prise en charge mais peut-être pas aussi étendue que chez les leaders (moins d'options pour la répartition des destinations, etc., ont été mentionnées).
- **Mobile et identifiants :** Feenics prend en charge les cartes/porte-clés traditionnels et a mis en œuvre l'OSDP pour des communications sécurisées avec les lecteurs. Pour l'accès mobile, Feenics lui-même n'avait pas d'identifiant mobile propriétaire en 2024 (pas d'intégration native Apple/Google Wallet et une fonctionnalité d'application mobile limitée pour les utilisateurs finaux). Cependant, étant basé sur Mercury, il peut utiliser les identifiants mobiles HID si des lecteurs HID sont utilisés, ou d'autres identifiants de lecteur BLE/NFC. L'accent de leur application mobile était davantage sur le contrôle administratif que sur le déverrouillage de porte par l'utilisateur final. C'est une faiblesse comparative en termes d'expérience utilisateur où les rivaux plus axés sur le mobile excellent.
- **Tableau de bord et expérience utilisateur :** Le tableau de bord web de Feenics est moderne mais a été cité comme ayant **moins de fonctionnalités** par rapport aux principaux concurrents. Il couvre l'essentiel : événements en direct, rapports, gestion des utilisateurs et configuration, mais pourrait manquer de certaines analyses avancées ou de composants d'interface utilisateur polis que d'autres vantent. Feenics permet des rapports personnalisés et dispose d'un moteur de règles pour l'automatisation de base. Un avantage est la capacité de gestion multi-locataires – un intégrateur peut gérer plusieurs sites clients à partir d'une seule interface, ce qui est excellent pour les fournisseurs de services gérés. Du point de vue du client final, il est simple pour le personnel de sécurité de l'utiliser pour les tâches quotidiennes.
- **Gestion des visiteurs :** Feenics d'ACRE comprend un système de **gestion des visiteurs natif**. Ils proposent une application de kiosque de gestion des visiteurs (VM) qui peut fonctionner sur une tablette pour l'auto-enregistrement. Cela se connecte à la plateforme Keep afin que lorsqu'un visiteur est enregistré, un identifiant temporaire puisse être émis et suivi. C'est une fonctionnalité intégrée intéressante, bien que, comme noté, le module de visiteur soit relativement basique selon les normes d'entreprise (enregistrement, impression de badge, notification de l'hôte).
- **Scalabilité :** Les solutions d'ACRE peuvent s'adapter aux niveaux d'entreprise. Keep (Feenics), étant basé sur le cloud, peut intrinsèquement évoluer horizontalement à mesure qu'AWS alloue des ressources. Le matériel Mercury sous-jacent peut gérer un grand nombre de lecteurs et de transactions (chaque panneau Mercury peut prendre en charge des dizaines de lecteurs et ces panneaux peuvent être mis en réseau). Par exemple, une seule instance Feenics pourrait gérer plusieurs sites avec des centaines de portes chacun. ACRE vend également toujours des systèmes sur site (comme Vanderbilt SMS ou RS2 AccessIT) pour ceux qui préfèrent un contrôle localisé ; ceux-ci sont également évolutifs mais avec les contraintes typiques de l'infrastructure serveur.
- **Sécurité et conformité :** ACRE en tant qu'entreprise ne publie pas beaucoup de certifications comme SOC 2 dans son marketing, mais étant donné que Feenics est hébergé sur AWS, il hérite de nombreuses conformités de sécurité d'AWS (ISO 27001, SOC 1/2 pour l'infrastructure). La plateforme utilise le chiffrement TLS pour toutes les communications et peut imposer la 2FA pour la connexion administrateur. On peut en déduire qu'ils effectuent probablement des audits de sécurité réguliers. Cependant, l'absence de mention explicite de la certification SOC 2 dans la documentation pourrait être une préoccupation pour certains clients (elle a été répertoriée comme un inconvénient par au moins un analyste, impliquant peut-être qu'elle n'avait pas encore obtenu certaines attestations de conformité). Côté matériel, les contrôleurs Mercury sont certifiés UL et compatibles avec le canal sécurisé OSDP, s'alignant sur les meilleures pratiques de l'industrie.
- **Tarification :** La structure de tarification d'ACRE pour Feenics Keep est généralement basée sur un abonnement par porte et par an. Le rapport de Genea a explicitement noté la « Tarification » comme un inconvénient sans élaboration, suggérant qu'elle pourrait être relativement élevée ou du moins non transparente. Les logiciels d'entreprise de Vanderbilt/RS2 ont souvent des frais de licence. Feenics vend probablement par l'intermédiaire d'intégrateurs qui fixent le prix final. Ainsi, bien que le matériel ouvert puisse réduire les coûts de réutilisation de l'équipement, le logiciel et le support pourraient toujours être significatifs. Il peut également y avoir des frais supplémentaires pour certaines intégrations ou applications mobiles (et en effet, Genea a noté que certains concurrents facturent un supplément pour les identifiants mobiles ; Feenics nécessitant éventuellement des abonnements HID pour les identifiants mobiles pourrait relever de cette préoccupation).

Points forts notables : La principale force d'ACRE est la **flexibilité et l'ouverture**. En utilisant le matériel Mercury sur bon nombre de ses produits, ACRE permet aux clients d'éviter le verrouillage fournisseur et de mélanger les composants. Si vous investissez dans un système ACRE et décidez plus tard de changer de logiciel, vos contrôleurs et lecteurs pourraient être réutilisés sous un autre système compatible Mercury (par exemple, Genetec ou Lenel). C'est un contraste frappant avec les systèmes propriétaires où un changement de plateforme signifie le remplacement de tout le matériel. Pour les organisations et les intégrateurs, cette atténuation des risques est précieuse. De plus, ACRE couvre *les deux* extrémités du spectre – du **cloud-first (Feenics)** au **sur site (Vanderbilt/RS2)** – afin que les clients puissent trouver une solution au sein de la famille qui correspond à leur philosophie informatique. En termes de fonctionnalités, les systèmes ACRE incluent toutes les capacités d'entreprise que l'on pourrait attendre : anti-passback basé sur les zones, contrôle d'ascenseur, configurations détaillées des règles d'accès, etc. La **gestion native des visiteurs** et les **fonctionnalités de confinement basées sur Mercury** sont des atouts pour les clients soucieux de la sécurité. Parce que les produits ACRE sont souvent livrés par des intégrateurs, ils sont accompagnés de **canaux de support robustes**, et la plateforme est conviviale pour les intégrateurs (par exemple, capacités multi-locataires pour les services gérés).

Inconvénients potentiels : Comparé à certains concurrents, les interfaces utilisateur et le niveau de finition d'ACRE pourraient être légèrement en retrait. La critique selon laquelle le tableau de bord a *« des fonctionnalités limitées par rapport à d'autres »* indique que l'expérience utilisateur pourrait être améliorée – peut-être que les rapports ne sont pas aussi élégants, ou que certaines commodités modernes (comme la planification par glisser-déposer ou les modifications groupées faciles) ne sont pas aussi fluides. De plus, bien que Feenics soit basé sur le cloud, il a été noté comme étant *« moins rationalisé que d'autres concurrents cloud non propriétaires »*, suggérant que des nouveaux venus comme Kisi ou Brivo pourraient actuellement offrir une expérience plus intuitive. Un autre inconvénient est le **manque de titres d'accès mobiles** – ACRE n'a pas sa propre application d'accès mobile pour les utilisateurs finaux (à la mi-2025, à notre connaissance). Cela signifie que les clients doivent s'appuyer sur des solutions mobiles tierces (par exemple, HID Mobile), ce qui peut ajouter des coûts et de la complexité (et en effet, une analyse de la concurrence a souligné l'absence de portefeuille Apple/Google et des fonctionnalités mobiles limitées comme des lacunes de Feenics). De plus, **certaines fonctionnalités nécessitent des frais ou des produits supplémentaires** – par exemple, le matériel/licence de borne visiteur, ou si l'on souhaite une intégration vidéo, il pourrait être nécessaire d'avoir un système vidéo Vanderbilt ou un VMS séparé, car la vidéo n'est pas incluse dans l'offre de base. Le prix étant quelque peu opaque et probablement plus élevé pour le cloud (en raison de l'orientation entreprise) peut être un frein pour les acheteurs sensibles au budget. Enfin, la gamme multi-marques d'ACRE peut elle-même être source de confusion – les clients potentiels pourraient ne pas savoir s'il faut implémenter Feenics ou Vanderbilt ACT, etc., sans consulter un intégrateur ACRE, alors qu'une entreprise mono-marque a une proposition plus claire. En résumé, les solutions d'ACRE sont puissantes et ouvertes, mais pas toujours les plus modernes en termes d'interface ou d'expérience mobile, ce qui les rend plus adaptées à ceux qui privilégient l'intégration et l'évolutivité plutôt qu'un design élégant.

5. Verkada

Présentation : Verkada est un nouvel acteur (fondé en 2016) qui s'est rapidement fait un nom dans le domaine de la sécurité physique grâce à son approche **tout-en-un, gérée dans le cloud**. Initialement connue pour ses caméras de sécurité connectées au cloud, Verkada s'est étendue au contrôle d'accès et aux capteurs environnementaux, se positionnant comme une plateforme unifiée de sécurité des bâtiments. L'offre de contrôle d'accès de Verkada, souvent appelée **Verkada Command for Access**, met l'accent sur le matériel plug-and-play, la **gestion centralisée dans le cloud** et une intégration étroite avec la vidéosurveillance. Elle cible les organisations qui souhaitent des systèmes modernes, adaptés à l'informatique et nécessitant une infrastructure minimale – Verkada se vante de ne nécessiter *« aucun serveur sur site »*. La solution est basée sur un abonnement, combinant le matériel (contrôleurs de porte intelligents) avec une licence logicielle qui couvre les mises à jour continues et le service cloud.

Fonctionnalités clés :

- **Architecture hybride-cloud :** Verkada utilise un modèle **« cloud hybride »** – les contrôleurs de porte (comme le contrôleur 4 portes Verkada AC41 ou l'interface de lecteur de porte AD32) gèrent les décisions en temps réel en périphérie, mais toute la gestion et les configurations sont effectuées via la plateforme cloud de Verkada (Command). Il n'y a *aucun serveur sur site* ; il suffit de connecter les contrôleurs à Internet et ils sont en ligne en quelques minutes. Si le réseau tombe en panne, les contrôleurs continuent d'appliquer l'accès en fonction de la dernière configuration connue (grâce au stockage/traitement local) et synchroniseront les événements une fois la connectivité rétablie (Source: verkada.com. Cela garantit une haute disponibilité et une résilience hors ligne.

- **Gestion cloud (Command) :** L'interface cloud Verkada Command est unifiée pour tous les appareils Verkada (caméras, portes, capteurs). Pour le contrôle d'accès, Command fournit une **application web et mobile** permettant aux administrateurs de gérer les utilisateurs, les horaires et de visualiser les événements. Elle présente un design extrêmement convivial, cohérent avec les applications SaaS modernes. Depuis n'importe quel navigateur, un administrateur peut glisser-déposer pour attribuer des portes à des groupes d'accès, définir des horaires de déverrouillage ou examiner un événement d'accès avec les séquences vidéo associées côte à côte. Command inclut des **plans d'étage visuels**, des répertoires d'utilisateurs centralisés et des règles d'alerte personnalisées (par exemple, alerter si une porte est forcée). L'application mobile permet de déverrouiller les portes en déplacement et de recevoir des notifications push.

- **Intégration vidéo et contexte :** La proposition phare de Verkada est l'**intégration native du contrôle d'accès avec la vidéo**. Si vous avez des caméras Verkada surveillant une entrée, la plateforme Command liera automatiquement les événements d'accès (déverrouillage de porte, ouverture/fermeture de porte, entrée refusée) au clip vidéo correspondant. Cela signifie qu'un agent de sécurité peut cliquer sur un événement d'accès et voir immédiatement qui a franchi la porte, améliorant considérablement la connaissance de la situation. Le système prend également en charge des analyses comme la **détection de talonnage** – utilisant l'analyse vidéo pour voir si deux personnes entrent avec un seul badge et signalant cela comme une alerte de talonnage. Verkada a également récemment ajouté un produit de **station de porte interphone**, entièrement intégré, de sorte que les appels interphones vidéo et les déverrouillages de porte via interphone s'intègrent au même système.

- **Titres d'accès mobiles et entrée sans contact :** Verkada prend en charge les titres d'accès mobiles basés sur le **Bluetooth Low Energy (BLE)** via son application Verkada Pass. Les utilisateurs peuvent déverrouiller les portes à l'aide de leur téléphone via l'application ou même configurer l'**entrée sans contact** : lorsqu'une personne s'approche, le lecteur Bluetooth peut détecter son téléphone et déverrouiller sans qu'il soit nécessaire de le sortir (c'est configurable). Ils ne prennent pas encore en charge Apple Wallet ou le tap NFC depuis le téléphone – cela se fait via l'application Verkada et le Bluetooth en arrière-plan. De plus, Verkada offre un support standard pour les badges/porte-clés, et de manière intéressante, peut également utiliser les **plaques d'immatriculation comme titres d'accès** dans certains scénarios (en lien avec leurs caméras LPR). Le système est flexible : toute combinaison de cartes, porte-clés, l'application smartphone de Verkada, ou même des **« liens de déverrouillage à distance »** (envoyer un lien à quelqu'un pour ouvrir une porte à distance) peut être utilisée.

- **Facilité d'installation et de migration :** Le matériel de Verkada est conçu pour la simplicité. Les contrôleurs sont alimentés par PoE et sont livrés avec des borniers à vis détachables pour le câblage des portes, ce qui rend l'installation simple pour les électriciens. Pour les rénovations, Verkada souligne que son contrôleur AC41 peut **fonctionner avec le matériel de porte et les lecteurs existants** – ce qui signifie qu'une organisation peut conserver ses gâches/aimants de porte et même ses lecteurs Wiegand si elle le souhaite, en ne remplaçant que le panneau de contrôle. Cela réduit les frictions de mise à niveau. Verkada dispose également d'une fonction pour importer les titulaires de carte et les titres d'accès existants via CSV ou s'intégrer via SCIM (par exemple, depuis Azure AD) pour intégrer rapidement les utilisateurs. Essentiellement, Verkada s'efforce de rendre le passage d'un système hérité aussi facile que possible, en tirant parti de la compatibilité lorsque cela est faisable (par exemple, les entrées de lecteur Wiegand).

- **Intégrations et API :** Verkada fournit un ensemble d'**API ouvertes, de webhooks et de SDK** permettant aux clients d'intégrer son système à d'autres logiciels. Il existe une API officielle de Verkada pour extraire des événements ou déclencher des actions, et ils prennent en charge **SCIM** (System for Cross-domain Identity Management) et **SAML SSO** pour l'intégration de répertoires d'utilisateurs. Par exemple, on peut intégrer Verkada avec Okta ou Azure AD pour gérer automatiquement les utilisateurs et les groupes d'accès. La **Marketplace** de Verkada présente des intégrations telles que la gestion des identités (par exemple, la synchronisation avec les bases de données RH) et Slack ou Teams pour les notifications. Ils ont également des webhooks qui peuvent notifier des systèmes externes d'événements. Comparé à certains systèmes plus anciens, l'approche d'intégration de Verkada est beaucoup plus moderne et adaptée à l'informatique.

- **Sécurité et conformité :** Verkada a investi massivement dans la sécurité du cloud. La plateforme et les produits ont obtenu la certification **SOC 2 Type II** et plusieurs certifications **ISO 27001/27017/27018** (couvrant la sécurité de l'information et la confidentialité du cloud). Verkada chiffre les données en transit et au repos, et de manière unique, parce que les séquences vidéo et certaines données sont stockées sur l'appareil et dans le cloud, ils mettent en œuvre une sécurité de bout en bout. Ils ont également introduit une option de **clé de chiffrement d'entreprise** où les clients peuvent détenir leurs propres clés pour les séquences vidéo (afin que Verkada ne puisse pas les visualiser – répondant aux préoccupations de confidentialité). Du point de vue de la confidentialité, Verkada prend en charge la conformité au RGPD et propose des fonctionnalités telles que des politiques de conservation des données et des journaux d'accès pour savoir qui a consulté la vidéo ou accédé aux données. Leur matériel est conforme à la NDAA (aucun composant interdit) et des modules de chiffrement certifiés FIPS 140-2 sont utilisés, répondant aux exigences gouvernementales. Ils subissent également des tests d'intrusion annuels et une surveillance continue de la sécurité.

- **Évolutivité et mises à jour :** Le système de Verkada est conçu pour évoluer – que vous ayez **10 portes ou 10 000 portes, sur des sites mondiaux**. Parce que tous les sites alimentent le même tableau de bord cloud, il est intrinsèquement adapté aux multi-sites. Il n'y a pas de limite supérieure pratique indiquée pour les lecteurs ou les utilisateurs ; Verkada fait régulièrement référence à des clients avec des dizaines de sites gérés de manière centralisée. La nature cloud signifie également des **mises à jour automatiques du micrologiciel et des fonctionnalités** – de nouvelles fonctionnalités sont déployées chaque mois sur la plateforme sans interruption, et les appareils reçoivent des mises à jour via Internet. Cela permet au système de s'améliorer au fil du temps sans projets de mise à niveau coûteux.

Points forts notables : La principale force de Verkada est l'**expérience unifiée et native du cloud**. Elle apporte la facilité de la technologie grand public à la sécurité d'entreprise. Les administrateurs informatiques apprécient qu'il n'y ait pas de DVR, de NVR ou de serveurs sur site à maintenir – il suffit de connecter le matériel et de tout gérer de manière centralisée. L'**intégration étroite de la vidéo et de l'accès** est un argument de vente majeur ; elle fournit un contexte aux événements d'accès sans effort et peut accélérer considérablement les enquêtes (par exemple, voir qui a suivi quelqu'un à travers une porte sans recouper manuellement la vidéo). L'interface utilisateur de Verkada est souvent saluée pour sa simplicité et son aspect moderne – une formation minimale est nécessaire pour que le personnel l'utilise. Un autre point fort est le **déploiement rapide** : l'ajout d'une nouvelle porte ou caméra peut être effectué en quelques minutes et apparaître dans le cloud, prêt à être configuré. Verkada s'étend également à de nouveaux domaines (capteurs environnementaux, alarmes, gestion des visiteurs avec Verkada Guest), tous alimentant une seule plateforme, ce qui est attrayant pour les clients souhaitant consolider leurs fournisseurs. D'un point de vue commercial, la **licence tout compris** de Verkada (matériel + garantie logicielle + support dans un seul prix) rend les coûts prévisibles et le support simple. Enfin, étant une entreprise technologique de la Silicon Valley, Verkada ajoute rapidement les fonctionnalités que les clients demandent (par exemple, ils ont introduit le **déverrouillage Face ID pour l'application mobile** et l'analyse de **détection de masque** pendant la période COVID, démontrant leur agilité). Il est considéré comme un **« système de sécurité simple et évolutif »** par des clients allant des écoles aux bureaux d'entreprise.

Inconvénients potentiels : L'approche de Verkada présente quelques réserves. Premièrement, il s'agit d'un **écosystème propriétaire** – vous devez en grande partie utiliser les contrôleurs et les logiciels de Verkada ensemble. Bien qu'ils permettent d'utiliser le matériel de porte et les lecteurs existants, le cerveau est celui de Verkada, et si vous quittiez Verkada, vous devriez probablement remplacer ces contrôleurs. C'est courant avec de nombreux systèmes, mais cela contraste avec les systèmes ouverts basés sur Mercury. De plus, les lecteurs de Verkada ne prennent actuellement pas en charge certains formats de cartes haute sécurité, sauf via des lecteurs tiers (leur contrôleur peut accepter Wiegand, mais leur propre lecteur est uniquement 13,56 MHz). Un autre inconvénient discuté dans certains cercles de sécurité était la **confidentialité** – au début, Verkada a eu un incident d'utilisation abusive interne (des employés visualisant des flux de caméras de manière inappropriée), que l'entreprise a résolu avec des contrôles plus stricts. Bien qu'ils aient depuis renforcé la confidentialité et le chiffrement, certaines organisations pourraient hésiter à placer une sécurité critique sur une plateforme cloud gérée par un tiers. De plus, le **coût de Verkada** peut être élevé : vous payez d'avance pour le matériel et une licence annuelle (généralement vendue par blocs de 5 à 10 ans). Sur une longue période, cela pourrait coûter plus cher que des solutions auto-gérées, bien que vous obteniez des mises à jour continues pour ce prix. Il y a aussi **moins de personnalisation** disponible par rapport aux systèmes traditionnels – vous opérez plus ou moins dans l'ensemble de fonctionnalités fourni par Verkada et attendez qu'ils implémentent de nouvelles fonctionnalités, par opposition à avoir des scripts personnalisés ou des modules tiers. Par exemple, une logique d'alarme avancée ou des intégrations en dehors de la portée de leur API pourraient ne pas être encore possibles. Verkada manque également de certaines fonctionnalités héritées comme l'*intégration d'annuaire actif pour le partitionnement basé sur les rôles* (ils font du SCIM pour le provisionnement des utilisateurs, mais les hiérarchies de rôles complexes pourraient être limitées). Et si un client a besoin d'une configuration matérielle spécifique que Verkada ne prend pas en charge (par exemple, des interfaces de tourniquet personnalisées ou des intégrations biométriques très spécialisées), il

pourrait être malchanceux car la gamme de produits de Verkada est encore en croissance (par exemple, seulement un certain nombre de types de contrôleurs, pas de contrôleur de tourniquet ou d'ascenseur natif, à l'exception de contournements de relais de base). Enfin, certains acheteurs pourraient ne pas aimer la **forte dépendance à la connectivité Internet** – bien que les contrôleurs fonctionnent hors ligne, l'administration dépend entièrement de l'accès au cloud ; dans des environnements hautement sécurisés ou hors ligne (par exemple, des installations classifiées), ce modèle pourrait ne pas être acceptable. En conclusion, Verkada excelle en simplicité et en intégration, mais ceux qui ont besoin d'une personnalisation extrême ou d'une autonomie hors ligne pourraient la trouver moins adaptée.

6. Brivo

Présentation : Brivo est un pionnier du contrôle d'accès basé sur le cloud, ayant lancé l'une des premières plateformes d'accès SaaS au début des années 2000. Leur produit phare, **Brivo Access (anciennement Brivo Onair)**, est un portail de gestion cloud associé aux contrôleurs matériels de Brivo sur site. Brivo a une forte présence sur le **marché intermédiaire et les déploiements multi-sites** tels que les chaînes de magasins, la gestion immobilière et les petites et moyennes entreprises. Ils proposent également des solutions complémentaires comme **Brivo Mobile Pass**, **Brivo Visitor**, et même une intégration vidéo native (caméras Brivo ou Eagle Eye Networks, les entreprises étant liées). Reconnue pour sa fiabilité et son innovation continue, Brivo offre une solution cloud mature avec des fonctionnalités robustes et des capacités d'intégration.

Fonctionnalités clés :

- **Plateforme de gestion cloud :** Brivo Access est une plateforme entièrement hébergée dans le cloud, accessible via un navigateur web et une application mobile. Elle gère très bien les sites multiples – les administrateurs peuvent gérer les portes, les horaires et les utilisateurs sur de nombreuses propriétés dans une seule interface. Le système fournit une surveillance en temps réel des événements, des déclencheurs d'alarme et la génération de rapports. Le tableau de bord de Brivo est considéré comme **convivial**, bien que certains l'aient trouvé légèrement moins moderne en termes d'expérience utilisateur que les interfaces des nouveaux venus. Néanmoins, il s'agit d'une **plateforme cloud éprouvée et stable** utilisée par des milliers d'organisations. Brivo propose également un **portail de services professionnels** permettant aux intégrateurs de gérer plusieurs sites clients de manière pratique.

- **Accès mobile et titres d'accès :** Brivo a été parmi les premiers à adopter les titres d'accès mobiles avec son **Brivo Mobile Pass**. Il s'agit d'une application qui permet aux utilisateurs de déverrouiller les portes via Bluetooth ou une commande Internet. De plus, Brivo s'est intégré à Apple Wallet – il offre la commodité de stocker un badge dans Apple Wallet pour un déverrouillage par tapotement avec iPhone/Watch. Cette intégration Apple Wallet est remarquable, car tous les systèmes ne la prennent pas encore en charge. L'application mobile de Brivo gère également les tâches *administratives* (pour les administrateurs autorisés) : par exemple, ils peuvent déverrouiller une porte à distance ou consulter les journaux d'événements sur leur téléphone. Une limitation notée est que les **titres d'accès mobiles au-delà d'un certain nombre peuvent entraîner des frais supplémentaires** – Brivo incluait historiquement un nombre limité de licences Mobile Pass par compte, et les licences supplémentaires coûtaient plus cher.

- **Matériel et infrastructure :** Les contrôleurs de Brivo (comme le Brivo ACS300, ACS6000) sont propriétaires mais construits sur une technologie ouverte (basée sur Linux). Les contrôleurs sur site se connectent au cloud de Brivo via Internet (via des connexions sortantes sécurisées, aucune connexion entrante n'est nécessaire). Le système utilise des modules de porte et des interfaces de lecteur qui peuvent évoluer de quelques portes à de grands bâtiments. **Compatibilité des lecteurs :** Le matériel actuel de Brivo prend en charge les lecteurs OSDP et Wiegand – de manière intéressante, Brivo s'associe à **Wavelynx** pour fournir la technologie de lecteur. Les lecteurs Wavelynx sont multi-technologies et permettent l'utilisation de Brivo Mobile Pass (via BLE). Cela signifie que si un client quitte Brivo, ces lecteurs pourraient devoir être remplacés car ils sont liés à cet écosystème. De plus, certains critiques soulignent que puisque Brivo fonctionne sur des panneaux propriétaires, passer d'un système Brivo signifie remplacer le matériel.

- **Intégrations et API :** Brivo dispose d'un **écosystème API robuste** et d'une **place de marché d'intégrations**. Ils s'intègrent aux **systèmes de gestion des identités** (Azure AD, Okta, G Suite), aux **applications CRM/Workspace** et aux systèmes de **sécurité physique**. Par exemple, Brivo peut s'intégrer à **Eagle Eye Networks VMS** pour fournir une vidéo liée aux événements d'accès (Brivo et Eagle Eye sont des sociétés sœurs). Ils ont également des partenariats pour la **gestion des visiteurs** (bien que Brivo ait aussi son propre module visiteur de base) et les systèmes de **contrôle d'ascenseur**. Une large gamme d'applications tierces – y compris les services d'annuaire, les plateformes d'analyse de données et même la domotique pour les versions résidentielles – peuvent se connecter à Brivo. Les clients et les développeurs tiers peuvent utiliser l'API REST de Brivo pour créer des solutions personnalisées (telles que la synchronisation des utilisateurs à partir d'une base de données RH ou le déclenchement d'événements de porte à partir d'une autre application).

- **Évolutivité :** Le cloud de Brivo est multi-locataire et a prouvé sa capacité à prendre en charge des déploiements à l'échelle de l'entreprise. Il est utilisé dans **plus de 20 millions de portes** (cumulées) selon certaines sources, et les déploiements uniques peuvent impliquer des centaines de sites. Une limitation signalée par les analystes est que l'interface de Brivo pourrait nécessiter plus de clics que nécessaire pour certaines tâches (comme la modification d'utilisateurs sur de nombreuses portes). Par exemple, l'ajout d'un utilisateur à plusieurs groupes pourrait impliquer la navigation dans plusieurs onglets, alors que d'autres systèmes pourraient avoir un flux de travail plus fluide. Mais en termes de capacité brute, Brivo peut gérer un grand nombre d'utilisateurs et de titres d'accès. Ils segmentent les fonctionnalités d'entreprise en éditions – par exemple, Basic, Standard, Enterprise – avec des fonctionnalités avancées (comme l'intégration SSO ou une utilisation accrue de l'API) disponibles dans les niveaux supérieurs.

- **Expérience utilisateur et applications :** Brivo propose différentes applications : **Brivo Mobile Pass** (pour les utilisateurs finaux déverrouillant les portes), **Brivo Access Mobile** (pour les administrateurs gérant en déplacement), et certaines applications spécialisées comme **Brivo Visitor**. Une critique est que Brivo avait historiquement plusieurs applications selon le cas d'utilisation. Par exemple, un utilisateur final utiliserait Mobile Pass, tandis qu'un responsable de la sécurité pourrait utiliser une application distincte pour l'administration. Des concurrents comme Kisi ou Genea se consolident en une seule application. Cette fragmentation peut dérouter les utilisateurs ou nécessiter plus de maintenance d'applications, bien que Brivo travaille à unifier les expériences. De plus, l'approche de gestion des visiteurs de Brivo (Brivo Visitor) exige que les invités téléchargent et se connectent à une application pour recevoir leur titre d'accès, ce qui peut être considéré comme peu pratique pour les visiteurs occasionnels – d'autres systèmes utilisent désormais des codes QR ou des liens SMS qui ne nécessitent pas de téléchargement d'application. Brivo a noté ces points faibles et pourrait faire évoluer l'expérience utilisateur en conséquence.

- **Sécurité et conformité :** Brivo possède de solides références en matière de sécurité. Il est **certifié SOC 2 Type II et ISO/IEC 27001:2013**, démontrant son engagement envers la sécurité des données. Ils détiennent également une attestation **CSA STAR Niveau 1** pour la sécurité du cloud. La plateforme de Brivo répond aux exigences du **RGPD** et ils fournissent de la documentation (support DPIA) pour les clients de l'UE. Ils sont également conformes au **CCPA/CPRA** en Californie. Pour les données de paiement (bien que non directement pertinentes pour le contrôle d'accès, sauf en cas d'utilisation du commerce électronique au sein du système), ils sont **conformes PCI-DSS**. Dans des secteurs verticaux comme la santé et l'éducation, Brivo peut prendre en charge les besoins de conformité **HIPAA** et **FERPA** par une configuration système appropriée. Leurs matériels et systèmes sont **conformes NDAA** (pas de composants chinois interdits) (Source: brivo.com. De plus, Brivo met l'accent sur la sécurité opérationnelle : ils disposent d'une **page de statut** publique pour la disponibilité du système et la redondance entre les centres de données. Dans l'ensemble, la posture de sécurité de Brivo est très robuste et bien documentée, ce qui est probablement un facteur expliquant pourquoi de nombreuses organisations sensibles font confiance à leur cloud.

- **Fonctionnalités avancées :** Parmi les fonctionnalités notables de Brivo Access, on trouve les **niveaux de menace actifs** (capacité de faire passer toutes les portes en mode confinement ou autres états avec une seule commande), l'**authentification multi-facteurs** pour les portes critiques (nécessitant un identifiant mobile plus un code PIN, par exemple), et des **tableaux de bord de données** qui peuvent afficher les tendances d'occupation ou les modèles d'utilisation des installations. Brivo a également introduit une fonction de **suivi d'occupation** pendant la pandémie pour surveiller le nombre de personnes via les passages d'accès. Pour les intégrateurs, Brivo propose des outils comme **Brivo Snapshot** qui capture et archive certains événements avec la vidéo associée. Ils prennent également en charge l'**Apple Watch** pour les déverrouillages via l'intégration Apple Wallet.

Points forts notables : La plus grande force de Brivo est sa **maturité dans le contrôle d'accès cloud**. Avec plus de 20 ans d'expérience dans le domaine, ils disposent d'une plateforme stable et fiable qui a été affinée par une utilisation intensive en situation réelle. Beaucoup considèrent Brivo comme la *référence absolue* pour l'accès cloud en termes de fiabilité et de sécurité. Le système offre un **ensemble robuste de fonctionnalités prêtes à l'emploi**, couvrant la plupart des besoins sans nécessiter de développement personnalisé. L'écosystème d'intégration de Brivo est riche – la capacité de s'intégrer nativement avec les **caméras Eagle Eye, les systèmes d'alarme, les services d'annuaire et les outils de gestion des visiteurs** en fait un choix polyvalent pour une gestion de sécurité unifiée. L'**intégration Apple Wallet** pour les identifiants est une force tournée vers l'avenir ; peu d'autres l'ont mise en œuvre de manière aussi transparente à grande échelle. De plus, Brivo propose des **options de tarification et des éditions évolutives**, ce qui le rend viable pour une petite entreprise avec quelques portes jusqu'à une entreprise avec des centaines de sites. Un autre avantage est l'**innovation continue** : ils ont maintenu la plateforme à jour avec des éléments tels que les contrôleurs de lecteurs de porte basés sur navigateur (afin qu'une réceptionniste puisse déverrouiller une porte depuis le web) et des fonctionnalités d'analyse. De plus, la **propriété et la confidentialité des données** : Brivo permet aux clients de posséder leurs données et fournit des exportations et des journaux pour la conformité, ce que certains écosystèmes plus fermés ne font pas aussi facilement. Leur longévité signifie également qu'un vaste réseau de revendeurs et d'installateurs certifiés est disponible pour soutenir les utilisateurs finaux dans le monde entier.

Inconvénients potentiels : Un inconvénient, noté dans les comparaisons, est que l'**interface utilisateur de Brivo peut être moins rationalisée** que celle de certains nouveaux venus. Les tâches peuvent impliquer plusieurs écrans et l'interface utilisateur, bien que fonctionnelle, pourrait sembler un peu datée ou complexe, en particulier dans l'ancienne interface Brivo Onair (la nouvelle interface Brivo Access a amélioré cela). Le problème des **applications multiples** est également un inconvénient – la gestion d'applications mobiles distinctes pour différentes fonctions peut entraîner de la confusion et des frictions pour l'utilisateur. Brivo a consolidé les fonctionnalités dans la plateforme Brivo Access pour atténuer ce problème. Un autre point concerne les **considérations de coût** : bien que Brivo ne publie pas ses tarifs, il y a souvent des coûts additionnels pour certaines fonctionnalités ou capacités. Par exemple, les **identifiants mobiles au-delà d'une petite allocation gratuite sont payants**, la gestion des visiteurs est un module additionnel, et l'intégration vidéo pourrait nécessiter des abonnements Eagle Eye. Ceux-ci peuvent s'accumuler et doivent être prévus. De plus, le **verrouillage matériel** est un facteur : les contrôleurs Brivo ne fonctionnent qu'avec le cloud de Brivo ; si un client souhaite un jour quitter Brivo, le matériel devrait être remplacé, ce qui est un engagement à considérer dès le départ. Certains utilisateurs ont également cité que le **support pour les personnalisations avancées** (comme le script personnalisé ou les cas d'utilisation inhabituels) est limité – vous le faites à la manière de Brivo ou pas du tout, en raison de la nature fermée du cloud. Enfin, la **solution de gestion des visiteurs de Brivo** exigeant qu'un invité télécharge une application est un désavantage concurrentiel à une époque où l'accès visiteur sans friction (codes QR) est préféré. Ils risquent de prendre du retard s'ils n'introduisent pas d'options d'enregistrement des visiteurs sans application (bien que les intégrateurs résolvent souvent ce problème en ajoutant des systèmes tiers et en les intégrant via API). En résumé, les inconvénients de Brivo concernent généralement l'UX et la flexibilité, plutôt que la capacité ou la fiabilité. Ils travaillent à moderniser l'interface, mais les nouveaux acteurs les surpassent parfois en élégance d'interface utilisateur. Néanmoins, pour beaucoup, les antécédents prouvés de Brivo l'emportent sur ces préoccupations.

7. Avigilon Alta (Motorola Openpath)

Présentation : Avigilon Alta est la solution de contrôle d'accès **Openpath** renommée sous Motorola Solutions (qui a acquis Openpath en 2023). Openpath était une startup disruptive offrant un matériel élégant et une plateforme d'accès cloud, axée sur le mobile, et sous Motorola, elle a été intégrée à l'écosystème cloud d'Avigilon. Avigilon Alta (Openpath) se concentre sur l'**accès mobile sans friction** et la gestion cloud facile, complétée par le portefeuille de sécurité vidéo de Motorola (caméras Avigilon Ava, etc.). Elle est connue pour son matériel magnifiquement conçu (lecteurs intelligents) et une approche conviviale pour les développeurs avant l'acquisition. Avigilon Alta est commercialisée comme une **solution d'accès premium et évolutive** qui peut fonctionner pour toute taille d'organisation, avec une force particulière dans les bureaux modernes et les entreprises souhaitant une sécurité flexible et connectée au cloud.

Fonctionnalités clés :

- **Accès mobile sans contact :** La renommée d'Openpath venait de la capacité des utilisateurs à s'approcher d'une porte et à la déverrouiller sans avoir besoin de sortir leur téléphone. Grâce à la fonction "Wave to Unlock" (Agiter pour déverrouiller) de l'application Openpath, un utilisateur peut agiter sa main près du lecteur et, via Bluetooth/infrarouge, le lecteur détecte le téléphone et déverrouille la porte. Cela offre une expérience d'**entrée mains libres**. De plus, les utilisateurs peuvent déverrouiller via un tapotement sur l'application ou l'application Apple Watch. Le système prend en charge les cartes-clés et les porte-clés comme sauvegarde, mais l'expérience mobile est primordiale. C'est un atout majeur pour les organisations souhaitant abandonner complètement les cartes. Il est à noter qu'**Openpath ne prenait pas en charge Apple Wallet ou Google Wallet** en 2025 (ce qui signifie que vous devez utiliser leur application, et non un identifiant de portefeuille natif) (Source: getgenea.com.

- **Plateforme Cloud :** Le logiciel cloud d'Avigilon Alta est un portail web et une application d'administration mobile qui permet une gestion complète du système depuis n'importe où. Il comprend la surveillance en temps réel de l'état des portes, la gestion des utilisateurs et les configurations d'alertes. L'interface est moderne, reflétant les racines de startup d'Openpath. Il prend également en charge les **liens d'accès invité**, où les administrateurs peuvent envoyer un lien temporaire ou un code QR à un visiteur pour lui accorder l'accès (sans que le visiteur n'ait besoin d'une application). La gestion multi-sites est intégrée, avec la possibilité de partitionner par site, tout en ayant des annuaires d'utilisateurs globaux. Le cloud est accessible mondialement et évolue sur une infrastructure robuste (Motorola l'a probablement migré vers son environnement cloud sécurisé).

- **Matériel et contrôleurs propriétaires :** Le système Avigilon Alta fonctionne avec des **contrôleurs et lecteurs propriétaires** développés par Openpath. Les contrôleurs (Openpath Smart Hubs) se connectent au matériel de porte, puis au cloud. Ils communiquent vers l'extérieur avec le cloud et peuvent fonctionner hors ligne en stockant les permissions localement. Les **lecteurs Openpath** sont des appareils élégants et multi-technologies qui gèrent le BLE, le WiFi et l'authentification mobile (et lisent également les cartes RFID standard 13,56 MHz). Le matériel est réputé pour sa facilité d'installation – les lecteurs sont discrets, utilisant souvent juste un câblage PoE basse tension. Comme il s'agit d'un écosystème matériel fermé, le passage à Alta nécessite l'utilisation de ces contrôleurs et lecteurs. L'avantage est que le matériel et le logiciel sont étroitement intégrés, garantissant une expérience utilisateur fluide et des déploiements rapides de fonctionnalités (par exemple, des mises à jour du firmware pour de nouvelles fonctions).

- **Intégration avec l'écosystème Motorola :** En tant que partie de Motorola, Avigilon Alta est intégré (ou en cours d'intégration) avec **Avigilon Ava Cloud Video** et les **plateformes Orchestrate et Ally de Motorola**. Cela signifie qu'un utilisateur d'Avigilon Alta peut voir les séquences vidéo des événements d'accès des caméras Avigilon dans la même interface, similaire à l'approche unifiée de Verkada. Motorola vante une "sécurité de bout en bout" – par exemple, en intégrant les alertes de porte Openpath avec l'analyse vidéo d'Avigilon (comme l'ouverture d'un flux de caméra lorsqu'une porte est forcée ou l'utilisation de l'IA de la caméra pour vérifier l'identité d'une personne à l'accès). L'intégration s'étend probablement également aux systèmes de radio et de communication d'urgence de Motorola pour la sécurité d'entreprise, bien que ces détails soient en évolution. Même avant l'acquisition, Openpath s'intégrait avec des VMS tiers comme Milestone et avec des systèmes d'alarme pour une sécurité holistique.

- **Permissions personnalisables et intelligence cloud :** Alta offre un contrôle d'accès granulaire basé sur les rôles, des plannings et même des restrictions basées sur les zones. Une fonctionnalité qu'Openpath possédait était le **suivi d'occupation** – en surveillant les entrées/sorties, le système peut évaluer le nombre de personnes dans un espace et appliquer la capacité si nécessaire (important pour la sécurité ou les politiques liées à la pandémie). Une autre est l'**accès basé sur des politiques**, comme l'exigence d'une double authentification sur certaines portes (le système prend en charge l'utilisation de l'application plus un deuxième facteur comme la biométrie ou une confirmation par interphone caméra). Des alertes en temps réel peuvent être définies pour les anomalies (porte laissée ouverte, tentatives multiples invalides, etc.). La nature cloud permet également des **mises à jour par voie hertzienne** qui ont historiquement ajouté des fonctionnalités comme le Confinement depuis n'importe où (un bouton de panique mobile qui verrouille toutes les portes), ou l'Anti-passback (bien qu'en tant que système plus récent, l'anti-passback n'ait peut-être pas été la priorité initiale, ils ont ajouté de telles fonctionnalités d'entreprise au fil du temps).

- **Gestion des visiteurs et accès invité :** Openpath n'avait pas d'application de gestion des visiteurs autonome, mais il facilitait l'accès des visiteurs grâce à ses liens de laissez-passer invité. Un administrateur ou un employé peut émettre un **laissez-passer invité** par e-mail ou SMS à un visiteur, ce qui fournit un lien que, lorsque le visiteur arrive, il peut taper et la porte se déverrouillera pour lui. Cela évite le besoin de télécharger une application (une commodité par rapport à la méthode de Brivo). De plus, Openpath s'intègre avec des systèmes de gestion des visiteurs populaires comme Envoy – lorsqu'un visiteur s'enregistre sur un iPad, Envoy peut déclencher Openpath pour lui envoyer un identifiant mobile pour la durée de sa visite. Cette capacité d'intégration pour la gestion des visiteurs est une force.

- **Intégrations tierces et API :** Openpath a été conçu avec l'ouverture à l'esprit (malgré son matériel propriétaire). Il dispose d'une **API REST** bien documentée et prend en charge les **webhooks**, permettant l'intégration avec des bases de données RH, des fournisseurs d'identité et d'autres services. Les intégrations prêtes à l'emploi incluent **Okta**, **Azure AD**, **Google Workspace** pour la synchronisation d'annuaire, **Slack** pour les notifications d'alerte et diverses plateformes d'analyse. Ils s'intègrent également avec **SAML SSO** pour l'authentification unique au tableau de bord d'administration. Une autre intégration est avec **IFTTT ou Zapier** – permettant des automatisations créatives comme allumer les lumières lorsque quelqu'un badge, etc., reflétant une approche axée sur la technologie.

- **Conformité et sécurité :** Motorola a veillé à ce qu'Avigilon Alta réponde aux normes de sécurité d'entreprise. Il a obtenu les certifications **SOC 2 Type II** et **ISO 27001** comme indiqué par le centre de confiance de Motorola. Il adhère également au RGPD pour la confidentialité des données (avec des options d'hébergement de données en région). Le matériel d'Openpath était **certifié UL 294** pour la sécurité du contrôle d'accès et conforme NDAA. Ils utilisent le chiffrement de bout en bout et offrent des fonctionnalités comme le **"Triple Unlock"** (trois méthodes de communication – BLE, WiFi, cellulaire – pour maximiser les chances qu'une porte s'ouvre même si un canal est hors service). Bien qu'Apple Wallet ne soit pas intégré, la sécurité de leur identifiant mobile est élevée, utilisant le déverrouillage biométrique du téléphone pour l'application et des échanges sécurisés de jetons cloud. Après l'acquisition, Motorola a probablement également intégré le produit dans ses processus de cryptographie validés FIPS 140-2. À noter, le cloud d'Openpath était hébergé sur Google Cloud Platform, connue pour son infrastructure fiable, mais sous Motorola, une partie du backend pourrait changer.

- **Tarification :** Openpath (Avigilon Alta) est vendu via des intégrateurs et des partenaires. Il facture généralement le matériel et un abonnement par porte par an pour l'accès cloud. Bien que non public, le prix était compétitif par rapport aux autres offres cloud premium. Ils mettaient souvent en avant le retour sur investissement lié à l'élimination des cartes-clés (car le mobile est inclus de manière illimitée). Une note importante : Openpath ne **facture pas par identifiant mobile** – n'importe quel nombre d'utilisateurs peut utiliser le système sans coût supplémentaire, ce qui est un différenciateur par rapport à certains modèles plus anciens. Cela encourage une adoption généralisée de l'accès mobile parmi les employés sans se soucier des frais supplémentaires.

Points forts notables : Avigilon Alta (Openpath) est particulièrement apprécié pour son **expérience utilisateur** – de l'élégance de taper sur son téléphone ou d'agiter pour déverrouiller, à l'interface d'administration épurée. Il offre une expérience très moderne qui correspond aux attentes des entreprises technologiques et des entreprises avant-gardistes. La fonctionnalité d'**accès sans friction** (Wave to Unlock) est un grand avantage pour la commodité et l'hygiène (un argument de vente pendant le COVID). L'intégration avec l'**écosystème Motorola** signifie désormais une solution combinée solide d'accès + vidéo + interphone, avec la fiabilité de Motorola derrière elle. Une autre force est la **vitesse d'innovation** : en tant que produit né d'une startup, Openpath a fréquemment publié des mises à jour et ajouté des capacités comme les commandes de confinement, le comptage d'occupation, etc., et cette culture peut se poursuivre sous Motorola. La conception matérielle est également un plus : les contrôleurs sont intelligents et les lecteurs sont attrayants (certaines entreprises choisissent Alta simplement parce que les lecteurs sont plus esthétiques dans leurs halls que les anciens lecteurs encombrants). L'**évolutivité et la gestion à distance** sont des forces inhérentes en tant que système cloud – la gestion multi-sites est facile et les changements globaux sont en temps réel. La capacité des administrateurs à utiliser une **application mobile pour les tâches d'administration** (l'application Openpath permet aux administrateurs d'effectuer des actions rapides et de voir les événements) est utile. En termes d'**intégrations**, Alta était parmi les meilleurs de sa catégorie, prenant en charge une variété d'outils de travail (par exemple, il s'intègre avec les **calendriers Office 365 et G Suite** afin que si une salle de réunion est réservée, il puisse accorder l'accès pendant ce créneau – une intégration unique pour la gestion de bureau). Enfin, faire partie de Motorola lui confère une stabilité financière et un soutien, apaisant les préoccupations antérieures que certains avaient concernant la longévité de la startup lorsqu'il s'agissait d'Openpath seul.

Inconvénients potentiels : Un inconvénient noté dans les analyses des concurrents était le manque de support pour Apple/Google Wallet (Source: getgenea.com – exiger l'utilisation de leur application pourrait être un obstacle pour certains utilisateurs qui préfèrent les badges de portefeuille natifs. Il y a aussi le **verrouillage matériel propriétaire** : vous devez utiliser leurs contrôleurs et lecteurs, ce qui pourrait être coûteux à remplacer initialement (bien qu'ils essaient de réutiliser le câblage et les serrures existants). Certaines grandes entreprises pourraient trouver quelques lacunes fonctionnelles par rapport aux acteurs établis : par exemple, **pas de mode hors ligne natif pour les sites sans internet** – il est dépendant du cloud (bien que vous puissiez le faire fonctionner sur une sauvegarde cellulaire). De plus, **pas de surveillance d'alarme intégrée** ; bien qu'Alta puisse s'intégrer aux systèmes d'alarme, il n'a pas son propre système d'intrusion (Verkada en a un, Brivo s'intègre étroitement avec alarm.com). Une autre considération est que, sous la marque Motorola, certains craignent si l'**ouverture restera** – historiquement, Openpath était assez ouvert en API, mais les grandes entreprises rendent parfois les produits plus fermés ; cependant, compte tenu des antécédents de Motorola, ils conserveront probablement les API. De plus, certains utilisateurs ont signalé que si le système est excellent quand tout va bien, le **dépannage des problèmes réseau ou matériels** peut être difficile car il dépend du cloud – par exemple, si un contrôleur se déconnecte, vous dépendez du support à distance ou de réparations sur site avec moins de contrôle local par rapport aux systèmes plus anciens (bien qu'il existe une option de clé physique de sécurité pour les portes si nécessaire). En termes de coût, Alta est une solution premium ; le matériel peut être plus cher que les panneaux Mercury génériques, et l'abonnement par porte est significatif (bien que comparable aux niveaux entreprise de Kisi ou Brivo). Enfin, comme pour toute acquisition, il pourrait y avoir des **problèmes de transition** – certains clients s'inquiétaient des changements de support ou de stratégie sous Motorola (par exemple, Motorola fusionnant Alta avec d'autres offres cloud comme Ava – mais jusqu'à présent, ils ont conservé "Alta" comme marque cloud, séparée de la ligne Avigilon Unity sur site). Tout bien considéré, les inconvénients d'Avigilon Alta sont relativement mineurs et typiques d'un système cloud propriétaire – ils tournent autour de l'assurance qu'il correspond aux préférences informatiques de l'organisation (propriétaire vs ouvert, application vs portefeuille, etc.) et de la budgétisation pour une solution haut de gamme.

8. Dormakaba

Présentation : Dormakaba est un leader mondial des serrures, de la quincaillerie de porte et des solutions d'accès physique. En matière de contrôle d'accès, Dormakaba propose à la fois des **systèmes d'entreprise** (comme leurs logiciels exos et MATRIX, la ligne Keyscan en Amérique du Nord) et des **solutions basées sur le cloud** (telles que Dormakaba exivo en Europe). La force de Dormakaba réside dans son vaste portefeuille de matériel – des serrures et lecteurs électroniques aux portes tournantes et tourniquets – et sa présence dans des secteurs verticaux comme l'hôtellerie, où il est un fournisseur dominant de serrures de porte d'hôtel. En tant que solution de contrôle d'accès commercial, Dormakaba offre une couverture de bout en bout : ils fabriquent les serrures/dispositifs de porte et le logiciel pour les gérer. Les offres de Dormakaba sont souvent adaptées à des besoins spécifiques (par exemple, leurs systèmes de serrures sans fil pour les universités, ou les systèmes sans clé pour le co-working). L'approche de l'entreprise met l'accent sur la **sécurité, la durabilité et l'intégration de l'accès mécanique et électronique**.

Fonctionnalités clés :

- **Solutions matérielles intégrées :** Dormakaba propose une **large gamme de matériel d'accès** qui peut tous s'intégrer à leurs systèmes. Cela inclut les lecteurs de cartes muraux traditionnels, les serrures de porte électroniques sans fil (compatibles RFID et BLE, souvent commercialisées sous le nom d'Orbis ou similaire pour les serrures autonomes), les **serrures à clavier** et les cylindres haute sécurité. Ils proposent également des systèmes d'entrée comme les **tourniquets, les portillons rapides et les portes tournantes** qui s'intègrent à leur contrôle d'accès. L'avantage est une solution à fournisseur unique pour tout, de votre barrière de parking à la porte de votre salle de serveurs. Par exemple, les serrures sans fil de Dormakaba peuvent être gérées en ligne via leur logiciel, réduisant le câblage lors des rénovations.

- **Plateformes logicielles :** Les logiciels d'entreprise de Dormakaba comme **Exos** (couramment utilisé en EMEA) ou **Keyscan Aurora** (populaire aux Amériques suite à l'acquisition de Keyscan par Dormakaba) offrent une gestion d'accès robuste sur site. Ces systèmes permettent une architecture client-serveur, des permissions basées sur les rôles, des plannings et l'intégration avec la vidéo/les alarmes. Exos est hautement évolutif, utilisé dans de grandes institutions et prend en charge des scénarios multi-locataires (comme les immeubles de bureaux multi-locataires). Dormakaba propose également des **applications mobiles pour l'administration** et les fonctions utilisateur dans certaines de ses offres, bien qu'historiquement, elles aient été davantage orientées client PC. Pour les PME et le cloud, **exivo** de Dormakaba est une plateforme cloud où les intégrateurs peuvent gérer l'accès pour plusieurs clients (particulièrement commercialisée en Europe pour les petites installations, permettant une gestion à distance par un fournisseur de services). Il est à noter que le portefeuille de Dormakaba est vaste et quelque peu fragmenté : différentes régions utilisent différents logiciels principaux (par exemple, aux États-Unis, les logiciels Keyscan Aurora et Smartspace ; en UE, exos et exivo ; dans l'hôtellerie, les systèmes Saflok/Ilco).

- **Identifiants mobiles :** Dormakaba prend en charge l'accès mobile via BLE dans bon nombre de ses serrures et lecteurs plus récents. Par exemple, leurs systèmes hôteliers Saflok permettent aux clients d'utiliser une clé de smartphone via BLE. Dans les systèmes commerciaux, Dormakaba propose des solutions mobiles (dont certaines exploitent des identifiants cloud ou des plateformes tierces). Par exemple, Dormakaba s'est associé à **Legic** et à d'autres pour des identifiants mobiles sécurisés. Cependant, l'adoption du mobile dans la sécurité générale (hors hôtellerie) a été un peu plus lente pour eux par rapport aux entreprises purement technologiques. C'est une fonctionnalité disponible, mais pas aussi centrale dans le marketing qu'avec Kisi ou Openpath. Cela dit, Dormakaba a introduit des fonctionnalités telles que le **provisionnement d'identifiants numériques** pour les sites distants et les **lecteurs Bluetooth** capables de lire des clés mobiles ou des clés Apple Wallet pour une utilisation hôtelière.

- **Gestion des visiteurs et modules haute sécurité :** Les systèmes d'entreprise de Dormakaba incluent souvent des **modules d'enregistrement des visiteurs** ou s'intègrent facilement à des systèmes de visiteurs tiers. Ils répondent également aux besoins de haute sécurité avec des modules comme le **badging (impression de cartes d'identité)**, la **ronde de gardien** et des flux de travail spécialisés (par exemple, la gestion des armoires à clés, l'intégration avec des systèmes de clés physiques – un clin d'œil à leur expérience en matière de clés mécaniques). Ils mettent l'accent sur les fonctionnalités de conformité comme les **pistes d'audit** et même l'**intégration biométrique** pour les zones nécessitant une authentification à deux facteurs (Dormakaba a acquis Stallings, une entreprise de lecteurs biométriques, il y a des années). Par exemple, leurs systèmes peuvent exiger une vérification d'empreinte digitale ou d'iris en plus du passage de carte pour certaines portes – utile dans les laboratoires ou les centres de données.

- **Évolutivité et orientation entreprise :** Les systèmes d'accès Dormakaba peuvent s'adapter à des milliers de portes et d'utilisateurs. Ils sont utilisés dans les **aéroports, les universités, les complexes de santé**, etc., où l'intégration de nombreux types de portes (câblées et sans fil) est nécessaire. Par exemple, un campus pourrait utiliser des serrures sans fil Dormakaba sur les chambres de dortoir, des lecteurs câblés sur les entrées principales et des tourniquets au gymnase – le tout géré sous un seul logiciel. Les systèmes sont généralement intégrés à des **systèmes d'entreprise comme SAP ou des bases de données RH**, synchronisant les statuts des utilisateurs. Exos de Dormakaba propose des fonctionnalités de **gestion des entrepreneurs** et d'**auto-enregistrement des visiteurs**, démontrant une orientation entreprise.

- **Intégrations tierces :** Le logiciel de Dormakaba peut s'intégrer aux **systèmes de gestion de bâtiment**, aux **systèmes d'alarme incendie** (par exemple, pour déverrouiller les portes en cas d'alarme incendie) et aux **contrôles d'ascenseur** (ils ont leurs propres cartes relais ou s'intègrent avec OTIS/Schindler, etc.). Ils proposent également des **API/SDK** pour leurs produits – par exemple, Keyscan Aurora dispose d'un SDK pour des intégrations personnalisées. Dans l'espace PropTech, Dormakaba travaille avec des entreprises comme **Altus et Spaceti** pour intégrer les données d'accès dans la gestion des espaces de travail. Et, en raison de leur orientation hôtelière, ils s'intègrent aux **systèmes de gestion immobilière (PMS)** comme Oracle Opera pour l'émission de clés aux clients d'hôtel.

- **Conformité et certifications :** En tant que grande entreprise, Dormakaba respecte les normes mondiales. Ils possèdent des certifications **ISO 27001** pour la sécurité de leurs informations dans certaines divisions (Source: dormakaba.com. Ils suivent probablement la norme SOC 2 en interne pour les offres cloud (exivo, etc.), bien que cela ne soit pas fortement médiatisé. Le matériel Dormakaba répond souvent à des certifications de sécurité strictes : **UL294, CE**, etc., et de nombreux produits sont certifiés **BSI (allemand) ou VdS** pour la haute sécurité. Ils mettent également l'accent sur la **conformité en matière de confidentialité** pour les services cloud. Dormakaba utilise un chiffrement sécurisé pour les identifiants (leurs cartes RFID utilisent généralement MIFARE DESFire sécurisé ou Legic advant). Ils se conforment également aux lois sur la protection des données si nécessaire – par exemple, exivo est hébergé dans des centres de données suisses pour les clients européens, en accord avec le RGPD. Une note de conformité intéressante : Dormakaba fournit des systèmes **certifiés TÜV** pour certaines applications gouvernementales, reflétant une profonde confiance dans leur sécurité.

- **Solutions sectorielles :** Dormakaba personnalise fortement ses solutions pour les différents secteurs. Dans l'**hôtellerie**, leur système d'accès est lié à l'enregistrement des clients, avec des fonctionnalités comme la planification de l'accès aux chambres, les passe-partout pour le personnel avec suivi, etc. Dans l'**immobilier commercial**, ils offrent un contrôle d'accès multi-locataires qui s'intègre aux annuaires des locataires et éventuellement aux systèmes de facturation. Dans l'**éducation**, ils ont des solutions pour gérer l'accès aux logements étudiants, s'intégrant aux bases de données étudiantes. Dans la **santé**, ils s'intègrent aux systèmes de sécurité infantile ou aux unités de distribution de pharmacie. Essentiellement, au-delà des fonctionnalités génériques, Dormakaba fournit des modules ou des partenariats adaptés pour répondre aux besoins spécifiques de l'industrie (comme la fonction de confinement pour les écoles, ou les serrures anti-ligature pour les établissements de santé comportementale). Cette personnalisation est une force clé de leurs offres.

Points forts notables : Le principal atout de Dormakaba est son **matériel complet et son expertise mondiale**. Peu d'entreprises peuvent offrir tout, du ferme-porte au logiciel de gestion d'accès électronique – Dormakaba le peut. Cela signifie une **intégration très fluide du matériel de porte physique avec le contrôle électronique** : par exemple, ils s'assurent que leurs serrures fonctionnent parfaitement avec leurs lecteurs en termes de fiabilité mécanique. Leurs solutions sont **éprouvées dans des environnements à fort trafic** (aéroports, grandes universités). Dormakaba est également à la pointe de la **technologie de verrouillage sans fil** ; eux et Assa Abloy ont largement été les pionniers des serrures sans fil, alimentées par batterie, qui se connectent à un système d'accès, ce qui est crucial pour la rénovation de bâtiments anciens (moins cher que de câbler chaque porte intérieure). De plus, leur **expérience dans l'hôtellerie** leur confère un avantage en matière d'expérience utilisateur pour certaines applications – par exemple, la gestion de l'accès temporaire des clients est quelque chose qu'ils font des millions de fois par jour dans les hôtels. Un autre point fort est le **support et la présence régionaux** : étant mondiaux, ils ont des bureaux locaux ou des partenaires dans presque tous les pays, ce qui est rassurant pour les entreprises multinationales qui souhaitent des systèmes standardisés. Dormakaba se distingue également par la **combinaison de la sécurité et de la commodité** – leurs systèmes ont tendance à offrir de nombreuses options de réglage fin (par exemple, vous pouvez définir des règles d'accès très spécifiques, des jours fériés, etc.) et intègrent des systèmes de clés mécaniques pour une approche holistique (comme lier les sorties de passe-partout physiques à la piste d'audit électronique). L'entreprise investit également en R&D autour des **nouvelles technologies** : par exemple, ils ont exploré l'utilisation de **clés intelligentes**, de **clés mobiles** et même de la **blockchain** pour les identifiants d'accès en concept. Enfin, la stabilité financière et la longévité de Dormakaba (issue de la fusion de Dorma et Kaba, chacune ayant plus d'un siècle d'existence) donnent confiance aux grands clients que le système sera pris en charge pendant des années et qu'il ne s'agit pas d'un produit d'une entreprise débutante.

Inconvénients potentiels : Un inconvénient peut être la **complexité et la nature cloisonnée** de leur portefeuille. Parce qu'ils ont plusieurs gammes de produits (Keyscan, exos, exivo, Saflok, etc.), il n'est pas toujours clair quel est « le système Dormakaba » que l'on devrait choisir, et ils ne sont pas tous unifiés. Un client pourrait se retrouver avec différentes plateformes Dormakaba pour différents cas d'utilisation (par exemple, un système hôtelier et un système de bureau d'entreprise distincts qui ne communiquent pas entre eux). Cette fragmentation peut également ralentir l'innovation ; un concurrent plus petit pourrait se mettre à jour plus rapidement qu'une grande entreprise coordonnant plusieurs gammes. En termes de convivialité logicielle, les interfaces de Dormakaba ont historiquement été **plus utilitaires** – elles fonctionnent bien mais peuvent sembler datées ou nécessiter plus de formation par rapport aux nouvelles interfaces utilisateur cloud élégantes. De plus, Dormakaba a été **plus lent à adopter pleinement le cloud à l'échelle mondiale** ; bien qu'exivo soit un produit cloud, son adoption est limitée à certaines régions et tailles de projets. De nombreux déploiements Dormakaba sont toujours sur site, ce qui convient à certains, mais d'autres peuvent y voir un retard par rapport à la tendance du cloud. Un autre inconvénient est le **coût** : le matériel Dormakaba est de qualité supérieure, et souvent tarifé en conséquence. Le coût total d'une solution intégrée Dormakaba (avec serrures sans fil, etc.) peut être élevé, bien que parfois compensé par des économies de main-d'œuvre (le sans fil signifie moins de coûts de câblage). De plus, l'**intégration avec des systèmes tiers** pourrait être moins "prête à l'emploi" que chez certains nouveaux venus – par exemple, une API existe, mais vous pourriez avoir besoin de l'aide de Dormakaba ou d'un revendeur pour écrire un script, alors qu'un SaaS moderne pourrait avoir des connecteurs plug-and-play. L'**expérience mobile** pour les utilisateurs finaux n'est pas aussi fluide que celles construites "mobile-first" (Openpath, Kisi, etc.), bien qu'ils la prennent en charge. Un autre inconvénient subtil : étant une entreprise axée sur le matériel, leur **modèle de support logiciel** passe souvent par des revendeurs/intégrateurs, de sorte que les temps de réponse ou l'innovation peuvent dépendre de cette chaîne, alors qu'une entreprise SaaS prend directement en charge le client final rapidement. Enfin, bien que Dormakaba couvre les bases comme SOC2 via des certifications ISO, ils ne le commercialisent peut-être pas fortement – certains acheteurs informatiques pourraient ne pas immédiatement considérer Dormakaba comme une « entreprise de logiciels » et être prudents quant à la sécurité du cloud, bien que la confiance soit probablement bien placée compte tenu de leurs certifications (Source: dormakaba.com. En substance, les inconvénients de Dormakaba sont typiques d'une grande entreprise établie : potentiellement moins agile, parfois moins axée sur l'utilisateur du côté logiciel, et un peu complexe à naviguer, mais aucun de ces éléments ne nuit à leur force principale qui est de fournir un contrôle d'accès solide et intégré.

9. Salto Systems

Présentation : Salto Systems est un fabricant espagnol réputé pour sa **technologie de verrouillage sans fil** innovante et ses solutions d'accès sans clé. Les produits Salto sont utilisés dans une variété d'environnements, des bureaux et espaces de coworking aux hôtels et grands campus. La marque de fabrique de Salto est la **capacité à mélanger et assortir des points d'accès hors ligne, sans fil et câblés** au sein d'un même système. Ils proposent une plateforme basée sur le cloud appelée **Salto KS (Keys as a Service)** pour gérer les serrures à distance, ainsi que des systèmes sur site comme **Salto Space** pour un contrôle plus localisé. Salto a été le pionnier du concept de « réseau virtuel » pour les serrures (SVN), où les serrures autonomes peuvent échanger des données via les identifiants des utilisateurs – une approche unique qui a précédé l'IoT mais en a réalisé de nombreux avantages. Cela permet un système hautement évolutif avec un câblage minimal. Salto se concentre sur la **flexibilité et les expériences sans clé conviviales**.

Fonctionnalités clés :

- **Serrures sans fil et intelligentes :** Le matériel de base de Salto comprend une grande variété de **formats de serrures électroniques** – des serrures cylindriques, des garnitures, des serrures à mortaiser, des cadenas, aux lecteurs muraux pour ascenseurs ou portails de parking. La plupart d'entre eux peuvent fonctionner sans fil (via BLE/Zigbee) ou de manière autonome (hors ligne). Leurs serrures stockent généralement les autorisations d'accès localement et prennent des décisions à la porte. La technologie **SVN (Salto Virtual Network)** de Salto permet aux serrures hors ligne de se mettre à jour et de recevoir des mises à jour via les identifiants des utilisateurs : par exemple, la carte d'un utilisateur peut récupérer une liste noire ou l'état de la batterie d'un lecteur en ligne et la transmettre aux serrures hors ligne sur d'autres portes lors d'une utilisation normale, réalisant ainsi une intelligence distribuée. De plus, Salto propose des **serrures sans fil en ligne** qui communiquent en temps réel via des passerelles, offrant des pistes d'audit en direct et des capacités de déverrouillage à distance instantanées. Cette diversité de formats de serrures rend Salto idéal pour les rénovations dans les bâtiments anciens ou les endroits où le câblage de chaque porte est peu pratique (comme les bâtiments historiques, ou pour couvrir des dizaines de portes dans un dortoir scolaire).
- **Plateforme Cloud (Salto KS) :** Salto KS est un système basé sur le cloud visant à offrir aux clients une gestion d'accès à distance via une application web ou mobile. Il est particulièrement populaire dans les espaces de coworking, les bureaux multi-locataires et les petites entreprises. Avec KS, les administrateurs peuvent émettre des clés numériques instantanément, révoquer l'accès en temps réel et surveiller les événements depuis n'importe où. L'application mobile pour Salto KS permet le déverrouillage des portes, ce qui signifie que les utilisateurs peuvent utiliser leur smartphone (avec l'application) pour déverrouiller les serrures Salto compatibles BLE. Il existe également une intégration d'**API cloud** pour connecter Salto KS à d'autres applications (comme les logiciels de planification ou la gestion des membres dans les espaces de coworking). Les fonctionnalités clés de Salto KS incluent la **gestion à distance de plusieurs sites**, le **partage de clés numériques par SMS/e-mail**, les **alertes en temps réel** et une interface élégante qui ne nécessite pas de connaissances techniques approfondies pour fonctionner. L'évolutivité est un point fort – Salto KS peut gérer un nombre illimité de serrures sur différents sites selon les besoins, puisque tout est dans le cloud.
- **Système sur site (Salto Space) :** Pour les entreprises qui préfèrent un contrôle local, Salto Space (avec le logiciel ProAccess SPACE) est leur outil de gestion sur site. Il permet une plus grande personnalisation, comme la **définition de groupes d'accès complexes, de fuseaux horaires et de jours fériés**. Il prend en charge le mélange de serrures en ligne et hors ligne. Avec Space, Salto offre des fonctionnalités comme **« JustIN Mobile »** – leur technologie de clé mobile – même pour les configurations sur site (les clés sont distribuées via un service cloud même si la gestion est sur site). Il fournit également des **intégrations** aux PMS (Property Management Systems) pour les hôtels, ou un accès à une **API/SDK** pour des intégrations personnalisées sur site. La solution sur site nécessite la mise en place de serveurs et est souvent livrée par les partenaires intégrateurs de Salto ; elle est robuste et utilisée dans de grandes institutions (sièges sociaux, universités, etc.).
- **Accès mobile :** Salto a été très performant en matière d'accès mobile, notamment avec **JustIN Mobile**. Les utilisateurs peuvent recevoir une clé mobile sur leur smartphone via l'application JustIN Mobile, qui utilise le BLE pour déverrouiller les serrures. Cette technologie est désormais largement utilisée dans les hôtels (les clients reçoivent leur clé de chambre sur leur téléphone) et de plus en plus dans les bureaux. Les clés mobiles sont chiffrées et peuvent fonctionner même hors ligne une fois téléchargées (elles contiennent les droits d'accès). Dans Salto KS, les déverrouillages mobiles se font via l'application KS, de manière similaire. De plus, Salto a mis en œuvre des fonctionnalités telles que le **Tap to Unlock via NFC** sur Android, et explorait les clés Apple Wallet (ils pourraient le prendre en charge pour certaines solutions hôtelières ou le feront bientôt, car Apple a ouvert cette possibilité à des tiers comme Assa Abloy et Dormakaba pour les hôtels). L'approche de Salto est d'offrir plusieurs options d'identifiants : vous pouvez utiliser des cartes (MIFARE, DESFire, etc.), des **porte-clés, des bracelets, des autocollants NFC**, des codes PIN (ils ont des serrures avec claviers) et des applications mobiles – ce qui la rend très flexible pour l'utilisateur final.
- **Intégrations tierces :** Grâce à l'API de Salto KS et aux capacités d'intégration de Salto Space, Salto s'intègre à de nombreuses plateformes. Dans le coworking, Salto KS s'intègre aux **plateformes comme Office RnD, Nexudus** (gestion des membres), permettant aux gestionnaires d'espaces d'automatiser l'accès lorsqu'un nouveau membre s'inscrit. Ils s'intègrent également à **Google Workspace et Microsoft 365** dans une certaine mesure (par exemple, en utilisant le calendrier pour ouvrir des salles de réunion). Pour les hôtels, Salto fonctionne avec tous les principaux systèmes PMS pour attribuer automatiquement l'accès aux chambres à l'enregistrement et le révoquer au départ. Salto s'est intégré aux **systèmes d'ascenseurs** pour permettre l'utilisation du même identifiant dans les ascenseurs (avec accès restreint aux étages). De plus, Salto a des partenariats pour la **gestion des visiteurs** – on peut envoyer une clé JustIN Mobile au téléphone d'un visiteur à l'avance, par exemple. Leur API

permet de récupérer les journaux et de gérer les utilisateurs à partir de programmes externes. Par exemple, un système d'information étudiant dans une université pourrait être lié de sorte que lorsqu'un étudiant s'inscrit, un identifiant Salto est créé, etc. Salto a également annoncé l'intégration avec les **caméras Cisco Meraki** pour une solution de sécurité intégrée (les journaux Meraki pourraient être liés aux événements de porte). Bien que moins publiquement annoncées que d'autres, ces intégrations rendent Salto très adaptable.

- **Sécurité et conformité :** La technologie de Salto utilise un chiffrement de haute sécurité (leurs cartes à puce utilisent AES 128 bits sur DESFire, etc., et les clés mobiles sont sécurisées de manière similaire). La certification ISO 27001 pour leurs opérations cloud confirme qu'ils maintiennent des pratiques solides en matière de sécurité de l'information. Ils ont réalisé un **audit SOC 2 Type II** comme mentionné dans l'un de leurs articles du centre d'aide, démontrant leur engagement envers la sécurité des données et les processus. Les données cloud de Salto KS sont souvent hébergées sur AWS dans des zones sécurisées, et ils se conforment au RGPD par conception (basés en Europe, ils sont attentifs à la confidentialité). Leur matériel est **certifié** – par exemple, de nombreuses serrures sont **classées EN pour le feu et la sécurité**, et certaines sont **certifiées BHMA** aux États-Unis pour la durabilité. Un aspect unique : comme de nombreuses serrures Salto sont alimentées par batterie, elles incluent des mesures de sécurité comme un avertissement lorsque la batterie est faible bien avant qu'elle ne s'éteigne (afin que vous puissiez la remplacer). Elles permettent également des dérogations d'urgence – des entrées de clé mécaniques ou des nœuds de démarrage rapide 9V – pour s'assurer que l'on ne soit pas bloqué en raison de problèmes d'alimentation. Ce ne sont pas des fonctionnalités de sécurité en soi, mais d'importantes fonctionnalités de sécurité opérationnelle. De plus, le système de Salto peut être configuré pour exiger une **authentification multi-facteurs à la serrure** (comme un code PIN + une carte sur certaines serrures équipées de claviers pour les zones de haute sécurité). Et ils prennent la conformité au sérieux en renouvelant l'ISO27001 et en s'alignant sur des normes comme les **Critères Communs** dans certains produits (pour les cas d'utilisation gouvernementaux nécessitant un équipement certifié).

Points forts notables : La principale force de Salto réside dans son **matériel polyvalent et son réseau hybride**. Dans un environnement comme une université ou un bureau moderne, Salto peut installer un accès électronique sur *chaque porte*, pas seulement celles du périmètre, car il n'est pas nécessaire de câbler chaque porte – c'est un avantage considérable pour étendre le contrôle d'accès électronique là où il était auparavant trop coûteux. L'**expérience utilisateur** est également une priorité : leurs serrures sont souvent élégantes (ils proposent des séries design pour s'adapter au décor), et des fonctionnalités comme la possibilité d'utiliser un bracelet au gymnase ou un téléphone au bureau offrent aux utilisateurs des options pratiques. La **scalabilité** est prouvée ; les installations Salto peuvent compter des milliers de serrures (par exemple, de grands systèmes de logement universitaire). Une autre force est la **capacité hors ligne** – parce que les serrures peuvent fonctionner de manière autonome et mettre en cache les données, une panne de réseau temporaire ou une panne de cloud ne compromettra pas immédiatement l'accès local ; les choses se synchroniseront plus tard. Pour Salto KS, la facilité d'inviter un utilisateur et d'accorder instantanément l'accès via le cloud est un grand avantage (comme l'envoi de clés numériques à distance). La forte présence de Salto dans l'industrie signifie qu'ils comprennent et proposent des fonctionnalités pour des scénarios spécifiques : par exemple, leur fonction d'occupation dans KS qui effectue un **suivi de l'occupation en temps réel** peut aider à mesurer l'utilisation de l'espace (pour les espaces de coworking ou les bureaux). Ils ont également introduit un mode **« Dérogation d'urgence »** où les portes peuvent être configurées pour s'ouvrir ou se verrouiller sur signal d'un système d'incendie, etc. La **communauté autour de Salto** – des intégrateurs du monde entier – est forte, de sorte que le support et les connaissances sont largement répandus. Enfin, Salto est reconnu pour son **innovation** : ils ont été parmi les premiers avec les clés de smartphone, et ils continuent d'innover (par exemple, en explorant récemment les serrures combinées BLE/WiFi, les intégrations cloud-to-cloud, etc.). Ils se soucient également des **données** – KS propose des analyses et des rapports qui peuvent montrer les modèles d'utilisation, aidant les entreprises à optimiser l'utilisation des espaces.

Inconvénients potentiels : Un inconvénient est la **dépendance aux serrures propriétaires** – si vous choisissez Salto, vous utilisez leurs serrures et cylindres. Bien qu'ils intègrent des lecteurs tiers, leur plein avantage réside dans l'utilisation des serrures Salto. Si l'on voulait mélanger Salto avec, par exemple, les serrures ou contrôleurs d'un autre fournisseur, ce n'est pas vraiment possible au niveau logiciel (bien que certains aient mis en place des configurations où Salto est utilisé pour les serrures intérieures et un autre système pour le périmètre, et ils synchronisent simplement les utilisateurs entre eux – mais c'est peu pratique). Un autre point est que **Salto KS, étant basé sur le cloud, dépend d'un abonnement**, ce que certains clients traditionnels refusent (ils préféreraient un achat unique ; Salto offre cependant cette option avec Space). Pour Salto KS spécifiquement, certaines fonctionnalités avancées des systèmes d'entreprise pourraient manquer – par exemple, un anti-passback de zone complexe, ou l'intégration avec les systèmes informatiques d'entreprise pourrait ne pas être aussi étendue (bien qu'elle couvre beaucoup via l'API). De plus, les **clés mobiles nécessitent l'application** – ce n'est pas un problème majeur, mais certains préfèrent l'approche du portefeuille natif, qui n'est pas encore pleinement utilisée en dehors de l'hôtellerie par Salto (bien qu'ils suivront probablement si l'industrie le fait). Bien que l'approche multi-technologique de Salto soit une force, elle peut également rendre le système **complexe à administrer** si vous avez un mélange de hors ligne et en ligne – vous devez gérer les niveaux de batterie, comprendre comment les données circulent via le réseau virtuel (une certaine courbe d'apprentissage pour ceux qui ne sont pas familiers). Leur mécanisme hors ligne (SVN), bien qu'ingénieux, signifie que si l'accès de quelqu'un est révoqué, il pourrait toujours y avoir accès jusqu'à ce qu'il présente sa carte à un dispositif de mise à jour en ligne ou que la serrure ait un délai d'expiration pour le cache – ainsi, la révocation immédiate n'est garantie que sur les serrures en ligne. Ils atténuent cela avec des temps de cache courts et en encourageant les gens à utiliser le mobile (qui se met à jour instantanément s'il est en ligne) ou la pratique de la mise à jour fréquente des cartes, mais c'est une considération – le **contrôle véritablement en temps réel** se fait sur les serrures sans fil en ligne ; pour le pur hors ligne, il y a un léger délai par nature. En termes d'interface utilisateur, Salto KS est bon, mais le logiciel sur site était historiquement perçu comme ayant une interface moins moderne (bien qu'il s'améliore). De plus, le **coût** : les serrures Salto ne sont pas bon marché ; chaque serrure de porte peut coûter plusieurs centaines de dollars, plus les coûts de logiciel/licence. Mais on pourrait soutenir que les économies de câblage et de main-d'œuvre compensent cela. Enfin, certains ont noté que le **support pour Salto peut varier selon les régions** – dans certaines zones, vous devez fortement vous fier au revendeur local pour le support (qui peut être excellent ou médiocre) car Salto est lui-même fabricant et ne supporte pas directement les utilisateurs finaux autant ; c'est typique dans l'industrie de la serrurerie. En résumé, les inconvénients de Salto sont liés à son approche unique (complexité hors ligne vs en ligne, nature propriétaire) et à la nécessité d'adapter les processus opérationnels de l'utilisateur à cela (comme le suivi des changements de batterie, etc.), mais ceux-ci sont gérables avec les meilleures pratiques.

10. Honeywell Commercial Security

Présentation : Honeywell est un conglomérat majeur avec une solide division de sécurité offrant des systèmes de contrôle d'accès, de vidéosurveillance et d'intrusion. En matière de contrôle d'accès, les offres phares d'Honeywell pour les entreprises incluent la **suite de sécurité Pro-Watch** et **WIN-PAK** (pour les PME), ainsi que *MaxPro Cloud* pour une approche hébergée. Les systèmes d'Honeywell sont largement utilisés dans les **projets à grande échelle tels que les aéroports, les installations gouvernementales et les campus d'entreprise**, ainsi que dans les bâtiments commerciaux de taille moyenne. Historiquement, les produits de sécurité d'Honeywell provenaient d'acquisitions (par exemple, Northern Computers/Win-Pak, puis la plateforme d'entreprise Pro-Watch, qui s'intègre avec le matériel propre à Honeywell et celui de tiers). La force d'Honeywell réside dans la fourniture d'une **solution de sécurité complète et intégrée** – ils lient souvent le contrôle d'accès à leurs **systèmes de gestion vidéo (par exemple, MaxPro VMS) et d'automatisation des bâtiments**. Ils sont connus pour leur matériel robuste et un réseau de partenaires établi.

Fonctionnalités clés :

- **Systèmes d'accès basés sur des panneaux :** L'approche traditionnelle d'Honeywell utilise des panneaux de contrôle (comme le N1000, le NS2, ou des contrôleurs modulaires plus récents) qui gèrent la connectivité des portes, connectés à un serveur sur site ou au cloud. **WIN-PAK** est un logiciel pour les installations de petite à moyenne taille, supportant jusqu'à des dizaines de portes et des dizaines de milliers d'utilisateurs. **Pro-Watch** est le logiciel d'entreprise, évoluant vers des centaines de sites et des milliers de portes. Ces systèmes offrent une surveillance en temps réel, la gestion des alarmes/événements et des rapports. Ils prennent en charge les **contrôleurs de porte génériques (basés sur Mercury)** dans les versions plus récentes (le propre matériel OEM d'Honeywell et les cartes HID Mercury), garantissant flexibilité et expansion facile. Les panneaux Honeywell sont assez standards en termes de câblage et de fonctionnalités, ce qui en fait une valeur sûre pour les installateurs.

- **Intégration et polyvalence :** La plateforme d'Honeywell est souvent décrite comme **polyvalente mais « fragmentée »** par certains, ce qui signifie qu'ils offrent de nombreuses pièces que vous pouvez combiner pour une solution. Par exemple, l'intégration vidéo : Pro-Watch peut s'intégrer aux **NVR MaxPro** d'Honeywell ou à DVM (Digital Video Manager) pour lier la vidéo aux événements d'accès. Ils peuvent également s'intégrer aux **panneaux d'intrusion d'Honeywell** (comme les séries Galaxy ou VISTA) pour l'armement/désarmement via les événements d'accès. Le système offre des fonctionnalités telles que des **cartes graphiques d'alarme**, des rapports de rassemblement, l'enregistrement des visiteurs et l'impression de badges d'identité nativement. Ils disposent d'un module natif de **gestion des visiteurs** et même d'une option de **borne d'accueil** – bénéfique pour les grands complexes.

- **Interfaces Web et mobiles :** Historiquement, une critique était qu'Honeywell manquait d'une interface web ou mobile élégante pour la gestion (l'ancien WIN-PAK était une interface utilisateur uniquement Windows). Cependant, les offres plus récentes comme **Pro-Watch 5.0 et WIN-PAK CS** ont introduit des composants client web et des applications mobiles (comme l'application *Honeywell Secure* pour la connaissance de la situation play.google.com, bien que cela puisse être plus axé sur la vidéo/alarme). Ils ont comblé cette lacune avec **MaxPro Cloud** – une plateforme où les panneaux plus petits (comme les contrôleurs de la série MB) se connectent au cloud et permettent la gestion à distance de l'accès et de la vidéo. Ceci est destiné aux petites entreprises multisites ou aux franchises pour gérer la sécurité à distance. Cela dit, leurs produits d'entreprise principaux utilisent encore souvent des logiciels clients lourds pour l'ensemble des fonctionnalités, ce qui peut être moins accessible à distance.

- **Scalabilité et fonctionnalités d'entreprise :** Honeywell Pro-Watch est utilisé dans certains des environnements les plus exigeants – par exemple, les aéroports où vous pourriez avoir des dizaines de milliers de titulaires de cartes, des intégrations avec des **badges PIV gouvernementaux** pour les sites fédéraux, et des exigences de haute disponibilité. Pro-Watch prend en charge les serveurs redondants, le clustering de bases de données et peut s'interfacer avec l'**Enterprise Buildings Integrator (EBI) d'Honeywell** pour la connexion au CVC, à la détection incendie, etc. Ils mettent l'accent sur la **« sécurité de niveau entreprise »** et disposent en effet de fonctionnalités telles que le chiffrement à tous les niveaux, des normes de titres sécurisés (ils prennent en charge les lecteurs OSDP, les nouvelles technologies de titres). La **gestion des titres** dans Pro-Watch peut être avancée – liaison aux annuaires d'entreprise, gestion des autorisations expirantes, etc. De plus, leurs systèmes gèrent des **cartes des plans d'étage en direct** où vous pouvez voir l'état des portes et les alarmes graphiquement, ce qui est utile pour les centres de contrôle de sécurité 24h/24 et 7j/7.

- **Sans cloud ou optionnel cloud :** Certains clients choisissent spécifiquement Honeywell parce qu'ils veulent un système sur site sans dépendance au cloud ou à la connectivité externe (par exemple, les secteurs gouvernementaux ou industriels). Honeywell répond à cela avec Pro-Watch/WinPak – qui peut être entièrement autonome, avec une intégration aux systèmes sur site. En même temps, pour ceux qui souhaitent la commodité du cloud (comme les intégrateurs offrant des services gérés), Honeywell propose l'édition **WIN-PAK CS (station centrale)** ou MaxPro Cloud qui permettent la gestion à distance par un revendeur ou un utilisateur. Cette flexibilité signifie qu'Honeywell peut répondre aux deux préférences. Cependant, un inconvénient historique est que le **cloud d'Honeywell est en retard** par rapport aux concurrents dédiés au cloud en termes de simplicité et d'expérience utilisateur (MaxPro Cloud était initialement plus axé sur la vidéo et basique pour l'accès).
- **Intégration matérielle et logicielle tierce :** Honeywell travaille avec plusieurs gammes de matériel. Ils ont leurs propres lecteurs **OmniAssure** pour les titres sécurisés, mais prennent également en charge HID, MIFARE, etc. Les systèmes peuvent utiliser des cartes Mercury, ce qui signifie que vous pourriez potentiellement changer de logiciel pour une autre plateforme compatible Mercury si nécessaire (bien qu'Honeywell essaie de vous maintenir dans son écosystème). En matière d'intégration logicielle, ils n'ont peut-être pas une API aussi ouverte que les nouveaux SaaS, mais Pro-Watch dispose d'un SDK et de connecteurs vers des systèmes comme **Lenel pour l'échange de données** (pour les grandes unifications d'entreprise). Historiquement, ils manquent d'intégrations directes aux systèmes RH prêts à l'emploi (que les nouveaux systèmes cloud vantent), mais les intégrateurs réalisent souvent des solutions personnalisées pour cela ou utilisent des outils d'importation. Notamment, l'accent mis par Honeywell sur la **conformité** se traduit par des fonctionnalités intégrées plutôt que de nécessiter une intégration : par exemple, des **rapports de conformité pour les réglementations SOX ou TSA** peuvent être générés directement dans Pro-Watch, ce dont un client du secteur financier ou de l'aviation pourrait avoir besoin.

Points forts notables : Le contrôle d'accès d'Honeywell est éprouvé pour les grandes **installations critiques**. Leurs systèmes gèrent des **scénarios complexes** – plusieurs sites, authentification multi-facteurs (ils prennent en charge nativement les lecteurs biométriques, et des choses comme exiger que deux personnes présentent des titres pour ouvrir une porte, etc.), et une intégration profonde avec d'autres systèmes de sécurité. L'**étendue de la solution** d'une seule entreprise est une force : ils peuvent fournir les **caméras (série 30, etc.), l'enregistreur (MaxPro), le système d'accès (Pro-Watch), et même le système d'alarme**, le tout lié. De nombreux directeurs de sécurité apprécient une solution intégrée unique. L'équipement d'Honeywell est également connu pour sa **longévité et son support** – certains systèmes Win-Pak fonctionnent depuis des décennies ; Honeywell offre des cycles de support à long terme (bien que parfois lents à mettre à jour les fonctionnalités). L'**infrastructure de support client** via Honeywell et ses revendeurs certifiés est solide à l'échelle mondiale. Une autre force est l'**expérience verticale** : ils ont des solutions/équipes dédiées à la **sécurité aéroportuaire, aux projets fédéraux, aux soins de santé** (avec des systèmes intégrés d'alerte enlèvement de nourrissons, etc.), etc. Ils savent comment répondre aux normes de conformité élevées (par exemple, Pro-Watch est conforme FICAM pour les normes fédérales américaines dès la sortie de l'emballage). La **stabilité et la fiabilité** des systèmes Honeywell sont souvent citées ; ils ne sont peut-être pas tape-à-l'œil, mais ils sont fiables – c'est crucial pour les installations qui ne peuvent pas se permettre de temps d'arrêt (comme un aéroport ne peut pas avoir son contrôle d'accès hors ligne – les systèmes Honeywell sont conçus pour fonctionner 24h/24 et 7j/7 avec des basculements). De plus, la **compatibilité ascendante** – Honeywell prend souvent en charge le matériel plus ancien dans les nouvelles générations de logiciels, facilitant les mises à niveau. Honeywell est également un leader dans certaines **technologies spécialisées** : par exemple, ils ont une solution intelligente d'**imprimante/encodeur de cartes à puce** qui s'intègre à Pro-Watch afin que vous gériez les badges de manière transparente. Et leur **présence mondiale** signifie un support linguistique local, la conformité aux réglementations locales (comme le RGPD, ils ont des modules pour aider à anonymiser les données personnelles dans les journaux si nécessaire), etc.

Inconvénients potentiels : Malgré l'offre d'options cloud, Honeywell a été perçu comme **en retard en matière d'innovation cloud-first**. Comme l'a noté le blog de Genea, c'est quelque peu **« fragmenté »** avec une architecture plus ancienne par endroits. Par exemple, pas d'expérience d'application mobile unifiée pour tout – certaines tâches nécessitent le client lourd, et l'utilisation mobile est limitée (manque d'une véritable plateforme de titres mobiles, bien qu'ils aient la capacité matérielle, la gestion n'est pas aussi transparente que chez certains nouveaux acteurs). En effet, Genea a souligné **« pas de plateforme d'accès mobile native – impossible de contrôler via smartphone »** comme un inconvénient (au moment de la rédaction). Ainsi, la convivialité en pâtit ; les petites organisations pourraient trouver Honeywell trop complexe à autogérer et s'appuieraient sur un intégrateur. Un autre inconvénient est que l'**orientation d'Honeywell vers les grands projets** signifie parfois que les petits clients se sentent mal desservis à moins de passer par un revendeur enthousiasmé par les services cloud. De plus, le **coût** peut être un problème : les solutions d'entreprise Honeywell sont réputées pour être coûteuses (licences logicielles propriétaires, contrats de support annuels, matériel haut de gamme). Et souvent, la **tarification n'est pas transparente** – vous devez passer par un processus de devis. Une autre plainte courante est la **bureaucratie du support client** – en tant que grande entreprise, les choses peuvent avancer lentement. De plus, parce qu'Honeywell fait tant de choses (des thermostats à l'aérospatiale), les clients s'inquiètent parfois de savoir si une ligne de produits spécifique (comme Win-Pak) reçoit suffisamment d'attention en R&D ; Honeywell a effectivement abandonné certaines lignes plus petites par le passé (comme la tentative de cloud NetAXS au début des années 2010 qui a été abandonnée). Mais compte tenu de leurs mises à jour continues de Pro-Watch/MaxPro, ils sont investis dans la sécurité. Enfin, **moins de capacités d'intégration modernes** – par exemple, l'intégration directe à Slack ou Teams pour les événements de porte n'est pas une fonctionnalité standard (bien que cela puisse être fait via certains services connectés). Ils manquent également généralement d'**intégration native d'annuaires (Okta/Azure)** pour le provisionnement des utilisateurs – ce qui signifie qu'il pourrait reposer sur une importation manuelle ou un travail personnalisé, ce qui est moins attrayant dans un monde automatisé. En résumé, les inconvénients d'Honeywell tournent autour de l'*expérience utilisateur (interface utilisateur plus ancienne, pas d'application unique pour tout), de l'agilité (moins rapide à adopter les nouvelles technologies à moins qu'elles ne soient éprouvées sur le marché), et du coût/complexité (frais généraux de niveau entreprise pour des besoins potentiellement plus simples)*. Pour un client averti en technologie souhaitant des interfaces élégantes immédiates et des mises à jour rapides des fonctionnalités, Honeywell pourrait sembler rigide. Cependant, pour ceux qui privilégient une fiabilité éprouvée et une intégration profonde dans un environnement complexe, ces inconvénients peuvent être des compromis acceptables.

Tableau comparatif des fonctionnalités

Le tableau ci-dessous compare les dix solutions selon les principales fonctionnalités et critères :

FONCTIONNALITÉ / CRITÈRE	KISI	JCI (C•CURE)	ADT	ACRE (FEENICS)	VERKADA	BRIVO	AVIGILON ALTA	DORMAKABA	SALTO	HONE
Gestion basée sur le cloud	Oui	Hybride (option Cloud)	Oui (via les applications ADT)	Oui	Oui (Source: verkada.com	Oui	Oui	Partiel (cloud exivo ; sur site aussi)	Oui (cloud Salto KS)	Hybri (MaxP Cloud site)
Accès mobile (App/Portefeuille)	Oui (App + Apple Wallet)	Partiel (HID Mobile via lecteurs)	Oui (App mobile et liens SMS)	Limité (pas natif ; HID via Mercury)	Oui (App, Bluetooth sans contact)	Oui (App Mobile Pass ; Apple Wallet)	Oui (App Openpath ; pas d'Apple Wallet) (Source: getgenea.com	Oui (JustIN mobile, serrures BLE)	Oui (App mobile JustIN)	Partie (lecte Omni suppo BLE ; d'app native
Matériel propriétaire vs ouvert	Contrôleurs propriétaires ; API ouverte	Mixte (panneaux propriétaires ; support Mercury)	Utilise divers (souvent Mercury/HID)	Ouvert (matériel Mercury)	Propriétaire (contrôleurs AC Verkada)	Propriétaire (panneaux Brivo ; lecteurs Wavelynx)	Propriétaire (contrôleurs/lecteurs Alta) (Source: getgenea.com	Serrures propriétaires, certaines intégrations Mercury	Serrures et lecteurs propriétaires	Panne propri (supp Mercu dans l nouve versio
Scalabilité (Portes et Sites)	Élevée (PME à entreprise mondiale)	Très élevée (campus d'entreprise)	Élevée (avec ADT Commercial pour les grands projets)	Élevée (évolue avec le cloud ; basé sur Mercury)	Élevée (10 à 10 000 portes)	Élevée (cloud multi-sites)	Élevée (cloud multi-sites)	Élevée (entreprise et hôtels)	Élevée (campus, grandes installations)	Très é (aérop gouv,
Gestion des visiteurs	Basique (codes QR, liens)	Oui (Module natif dans C•CURE)	Intégré aux alarmes/interphone (ADT propose des solutions)	Oui (VM natif et borne)	Verkada Guest (visiteur intégré)	Oui (Brivo Visitor ; app requise)	Via liens invités ou intégration Envoy	Oui (options visiteurs, notamment hôtels)	Via intégrations (applications de coworking)	Oui (V natif d Pro-W
Alertes et journaux en temps réel	Oui (journaux en direct, alertes personnalisées)	Oui (consoles de surveillance 24/7)	Oui (alertes via app/SMS)	Oui (tableau de bord cloud + rapports)	Oui (alertes instantanées + contexte vidéo)	Oui (alertes, rapports robustes)	Oui (événements cloud en temps réel)	Oui (journalisation de niveau entreprise)	Oui (temps réel avec serrures sans fil en ligne)	Oui (g riche alarm dans l
Permissions/Rôles personnalisés	Oui (basé sur les groupes, horaires)	Oui (très granulaire, RBAC d'entreprise)	Oui (flexible via personnalisation)	Oui (groupes, rôles, basés sur le temps)	Oui (groupes d'utilisateurs, SCIM pour les rôles)	Oui (rôles d'administrateur multi-niveaux)	Oui (rôles et rôles d'administrateur cloud)	Oui (granulaire dans le logiciel)	Oui (granulaire, contrôle de zone)	Oui (n de privilè étend
Capacités de déverrouillage à distance	Oui (via web/app cloud)	Partiel (via client lourd ou nouveau module web)	Oui (app ADT ou centre d'appels)	Oui (admin cloud ou mobile)	Oui (app/web Command)	Oui (portail web et admin mobile)	Oui (tableau de bord cloud ou app)	Oui (pour serrures en ligne ; hors ligne via mise à jour)	Oui (app Salto KS ou commande logicielle)	Partie (nouv modu web perme un cer contrô plus a via cli

| **Intégrations tierces** | Oui (plus de 20 intégrations : AD, Slack, etc.) | Oui (vidéo, alarmes, identité via SDK) | Oui (écosystème de sécurité, personnalisable via l'intégrateur ADT) | Oui (Workday HR, Okta, etc.) | Oui (API, webhooks, SCIM, intègre la vidéo) | Oui (API ouverte, Eagle Eye VMS, Envoy) | Oui (Okta, Envoy, G Suite, Slack) | Oui (PMS pour hôtels, BMS, etc.) | Oui (logiciels de co-working, PMS, etc.) | Oui (vidéo, CVC, synchronisation d'identité via SDK) | | **Certifications de sécurité** | SOC 2, ISO 27001, GDPR | Compatible SOC2 (cloud sur AWS), FIPS 201 | – (S'appuie sur les fournisseurs sous-jacents ; surveillance ADT certifiée UL) | – (Non public, mais basé sur AWS ; matériel Mercury) | SOC 2, ISO 27001/17/18 | SOC 2 Type II, ISO 27001 | SOC 2, ISO 27001+ (centre de confiance Motorola) | ISO 27001 pour le cloud (Source: dormakabagroup.com | SOC 2 Type II, ISO 27001 | – (Probablement SOC2 via audit interne, non promu publiquement ; normes de sécurité d'entreprise) | | **Transparence des prix** | Élevée – fourchette publiée (matériel et abonnement) | Faible – sur devis (licences d'entreprise) | Moyenne – forfaits avec surveillance, sur devis | Moyenne – via revendeurs ; prix d'abonnement disponibles | Moyenne – prix standardisés via représentants (le TCO inclut la licence par appareil) | Moyenne – via revendeurs ; connu pour facturer certains extras | Moyenne – via intégrateurs, niveaux de prix connus mais non publics | Faible – devis du revendeur ; varie selon la taille du projet | Moyenne – Salto KS propose des niveaux d'abonnement simples en ligne | Faible – devis personnalisés pour chaque déploiement | | **Solutions spécifiques à l'industrie** | Oui (coworking, fitness, bureaux) (Source: getkisi.com | Oui (gouvernement, entreprise, aviation) | Oui (commerce de détail, PME, franchises multi-sites) | Non explicite, mais axé sur l'entreprise (technologie, immobilier commercial) | Oui (cas d'utilisation présentés pour l'éducation, le commerce de détail, le gouvernement) | Oui (multi-logements, commercial, églises, etc.) | Oui (bureaux, multi-logements, campus technologiques) | Oui (leader de l'hôtellerie, aéroports, etc.) | Oui (hôtellerie, éducation, co-working) | Oui (aéroports, santé, industrie) |

Notes du tableau : "Partiel" indique que la fonctionnalité est disponible mais avec certaines limitations ou par des moyens tiers. Un blanc/"–" signifie non explicitement applicable ou non mis en avant. Les capacités de chaque solution sont citées à partir des sources : par exemple, les atouts d'intégration et mobiles de Kisi, la conformité cloud de Johnson Controls, les certifications de Brivo, etc. Cette matrice souligne comment les nouvelles solutions cloud (Kisi, Verkada, Brivo, Openpath) excellent en matière de convivialité mobile et de simplicité, tandis que les systèmes traditionnels (Johnson, Honeywell) brillent par leur intégration sur site à grande échelle mais s'adaptent aux attentes du cloud. Les acteurs de milieu de gamme (Feenics d'ACRE, Dormakaba, Salto) offrent une flexibilité spécialisée – ouverture Mercury, serrures sans fil – répondant à des besoins uniques sur le marché.

Conclusion et recommandations par cas d'utilisation

En 2025, le paysage des solutions de contrôle d'accès commercial s'étend des jeunes pousses natives du cloud aux vénérables plateformes d'entreprise. Le "meilleur" choix dépend fortement de la taille de l'organisation, de son secteur d'activité et de ses exigences de sécurité spécifiques. Ci-dessous, nous concluons par des recommandations personnalisées pour divers cas d'utilisation courants :

- **Petite entreprise (Bureau unique ou magasin de détail) :** Pour les petites entreprises ou les points de vente qui ont besoin d'un système convivial et abordable, **Kisi** est un excellent choix. Sa gestion basée sur le cloud et ses identifiants mobiles faciles nécessitent un minimum de frais généraux informatiques, et la tarification est transparente pour la budgétisation. **Brivo** est un autre concurrent sérieux ici, offrant une plateforme cloud éprouvée avec une gestion à distance robuste et une intégration à la surveillance des alarmes (via des partenaires) – idéal si vous souhaitez un système simple installé et éventuellement surveillé par un fournisseur de services. Si une installation professionnelle et un support continu sont préférés, **ADT** peut concevoir un forfait qui comprend non seulement le contrôle d'accès, mais aussi les alarmes anti-intrusion et les caméras dans un seul ensemble. Pour les très petits budgets ou les inclinations DIY, certains pourraient envisager l'offre cloud d'ADT ou l'offre d'accès de SimpliSafe, mais celles-ci manquent des fonctionnalités plus riches de Kisi ou Brivo. Dans l'ensemble, **Kisi** est souvent privilégié pour les petites entreprises en raison de sa facilité d'utilisation, de son intégration avec G Suite/Office 365 et de son coût de démarrage modeste (pas de serveurs, faible encombrement matériel).

- **Entreprise de taille moyenne (PME en croissance, bureaux multiples) :** Les organisations de taille moyenne avec des dizaines d'employés et peut-être plusieurs sites de bureaux devraient considérer **Brivo** et **Openpath (Avigilon Alta)** comme des options de premier ordre. **Brivo Access** fournit un tableau de bord cloud centralisé pour gérer plusieurs bureaux, avec des fonctionnalités telles que les identifiants Apple Wallet et un éventail d'intégrations (gestion des visiteurs, services d'annuaire) qui conviennent à une entreprise en croissance. **Avigilon Alta (Openpath)** séduit les entreprises axées sur la technologie – son expérience mobile-first et sans contact impressionnera les employés et son intégration avec la sécurité vidéo (sous Motorola) peut couvrir des besoins de sécurité plus larges. Les deux permettent une mise à l'échelle facile vers de nouveaux bureaux en installant simplement plus de contrôleurs de porte qui se connectent au cloud. **Salto KS** est un excellent choix si les bureaux de l'entreprise ont de nombreuses portes intérieures ou des formats de serrures uniques (les serrures sans fil de Salto peuvent sécuriser les salles de serveurs, les armoires, etc., sans câblage) – de plus, l'API cloud de Salto KS peut s'intégrer aux applications de travail pour la réservation d'espaces et autres. Les entreprises qui préfèrent une approche sur site mais souhaitent toujours une facilité d'utilisation pourraient opter pour **Honeywell WIN-PAK ou NetAXS** pour un seul bâtiment (bien que ceux-ci manqueront de certaines commodités du cloud) – cependant, compte tenu de la tendance, un système cloud comme Brivo ou Openpath offre généralement plus de valeur et une gestion multi-sites plus facile dans cette catégorie. Pour les entreprises de taille moyenne, **Kisi** est également viable, surtout si elles apprécient une configuration rapide et une large intégration (Kisi peut s'adapter à des dizaines de portes dans plusieurs bureaux avec un contrôle cloud global, et sa tarification reste raisonnable à mesure que vous grandissez).

- **Siège social ou campus d'entreprise :** Les entreprises exigent souvent une intégration avec l'informatique d'entreprise, une évolutivité élevée et des contrôles de sécurité avancés. **Johnson Controls C•CURE 9000** est un choix de premier ordre pour les grands sièges sociaux ou les environnements de campus nécessitant une personnalisation étendue – il excelle dans la gestion d'un grand nombre d'utilisateurs, de jeux de règles complexes et l'intégration dans les écosystèmes d'entreprise (comme LDAP/AD, murs vidéo, systèmes d'incendie). Les entreprises qui disposent d'un support informatique robuste et peut-être de systèmes hérités existants pourraient se tourner vers **Honeywell Pro-Watch** ou **Lenel (non inclus dans la liste des 10 meilleurs mais un autre système de niveau entreprise similaire)**, mais parmi nos 10 meilleurs, Johnson Controls se distingue par son classement et ses fonctionnalités pour les entreprises. Cependant, de nombreuses entreprises envisagent désormais des modèles cloud-hybrides : **Avigilon Alta (Openpath)** sous Motorola Solutions pourrait être proposé même à l'échelle de l'entreprise, en particulier aux entreprises technologiques ou à celles qui modernisent leurs campus – il offre une sécurité de niveau entreprise (cloud certifié SOC2, ISO) avec une expérience utilisateur (mobile, cloud) bien supérieure à celle des systèmes plus anciens. En fait, le mélange de solutions est également une stratégie : par exemple, utiliser **C•CURE** pour la sécurité de base contrôlée par le personnel de sécurité, mais superposer **Openpath** ou **Kisi** pour une gestion flexible des suites de bureaux par l'équipe informatique ou l'équipe du lieu de travail – cependant, un tel mélange est complexe. Si une entreprise valorise le **matériel ouvert Mercury**, elle pourrait choisir une solution ACRE (Feenics) pour maintenir le matériel standard et le logiciel basé sur le cloud. En fin de compte, les entreprises dotées d'opérations de sécurité dédiées ont tendance à privilégier **Johnson Controls (Software House)** ou **Honeywell** pour leurs antécédents éprouvés, mais les entreprises tournées vers l'avenir adoptent de plus en plus **Verkada** ou **Openpath** lorsqu'elles rénovent leurs bureaux, car ces solutions offrent une évolutivité plus facile sur de nombreux sites à l'échelle mondiale et s'intègrent à d'autres services (les caméras de Verkada, par exemple, simplifient le déploiement vidéo dans toute une entreprise). Pour les entreprises de bureaux purs, **Verkada** peut être recommandé en raison de sa gestion centrale simple et de la surveillance intégrée – les services informatiques apprécient de ne pas avoir à maintenir de serveurs et le provisionnement rapide des utilisateurs via SCIM.

- **Espaces de co-working et bureaux flexibles :** Ces environnements exigent un mélange d'**évolutivité, d'intégration avec la gestion des membres et de partage d'accès fluide**. **Salto KS** s'est fait un nom dans les franchises de co-working et de bureaux flexibles ; ses connexions API avec les logiciels de co-working (comme Nexudus, OfficeR&D) automatisent l'octroi d'accès lorsqu'une adhésion est active. Ses serrures sans fil permettent aux opérateurs de co-working de sécuriser facilement les bureaux privés et les salles de réunion, tandis que la gestion cloud gère les opérations multi-sites. **Kisi** est un autre excellent choix ici – Kisi a ciblé le co-working dans son marketing et ses fonctionnalités (comme le partage facile de liens invités, l'intégration avec les systèmes de calendrier pour déverrouiller les salles de réunion selon un horaire) (Source: getkisi.com. En fait, un certain nombre de chaînes de co-working ont déployé Kisi pour sa facilité d'utilisation et le fait que les membres peuvent utiliser des cartes mobiles ou NFC de manière interchangeable. **Openpath (Avigilon Alta)** convient également bien au co-working : les fonctionnalités Wave-to-Unlock et de laissez-passer invité créent une expérience haut de gamme et transparente pour les membres et les visiteurs. La gestion cloud permet aux gestionnaires de communauté d'administrer l'accès à distance et en temps réel. Brivo pourrait également être utilisé, bien que l'approche visiteur de Brivo nécessitant une application puisse être une légère friction pour les invités de passage – néanmoins, l'intégration de Brivo avec des applications comme **Kisi (via Envoy)** ou directement couvrirait l'enregistrement des visiteurs avec des codes QR. Compte tenu du top 10, **Salto KS** et **Kisi** obtiennent les meilleures recommandations pour le co-working en raison de la profondeur de l'intégration et de l'accent mis sur la gestion multi-espaces ; **Openpath** est un proche troisième pour son expérience utilisateur élégante qui peut être un argument de vente pour les marques de co-working premium.

- **Établissements de santé (Hôpitaux, laboratoires) :** Le secteur de la santé exige la conformité (HIPAA, souvent les normes de sécurité JCAHO) et un mélange d'accès hautement sécurisé et flexible (crèches vs. zones publiques). **Honeywell Pro-Watch** ou **Johnson Controls** sont bien adaptés aux grands campus hospitaliers – ils s'intègrent aux systèmes de prévention d'enlèvement de nourrissons, aux armoires pharmaceutiques et peuvent mettre en œuvre des pistes d'audit strictes. Ils gèrent également l'authentification multi-facteurs aux portes sensibles (par exemple, exigeant un code PIN ou une biométrie pour les salles de médicaments). Cependant, pour les petites cliniques ou laboratoires, une solution cloud plus simple pourrait suffire : **Brivo** ou **Kisi** peuvent fournir la sécurité nécessaire avec moins d'infrastructure, et ils prennent tous deux en charge les intégrations avec les services d'annuaire pour gérer facilement l'accès du personnel à mesure que le personnel change. **Dormakaba** excelle dans le secteur de la santé où il existe de nombreuses portes intérieures – ses serrures sans fil peuvent sécuriser les salles de dossiers patients, les armoires à médicaments, etc., sans câblage, et Dormakaba propose des solutions spécifiques pour la santé (ils mentionnent l'utilisation industrielle et sanitaire). Ils proposent également du matériel de qualité hospitalière (serrures avec revêtement antibactérien, etc.). Ainsi, pour un grand hôpital avec une commande de sécurité unifiée, **Honeywell** ou **Johnson (Software House)** est recommandé pour leur approche complète et leurs outils de conformité. Pour un établissement de santé plus petit ou un réseau de cliniques, **Brivo** avec son cloud et sa position prête pour HIPAA (ils mentionnent même le support de la conformité HIPAA) pourrait être un choix solide, offrant une surveillance à distance sur tous les sites. **Verkada** fait également des percées dans le secteur de la santé grâce à sa vidéo intégrée – les directeurs de la sécurité apprécient de voir qui a accédé à une armoire de pharmacie immédiatement via une caméra liée, par exemple. Mais attention dans le secteur de la santé : assurez-vous que le système est conforme à la NDAA (la plupart des 10 premiers le sont) et sécurisé du point de vue de la cybersécurité (SOC 2, etc., ce que Kisi, Brivo, Verkada sont tous).

- **Établissements d'enseignement (Écoles et universités) :** Les écoles privilégient la sécurité des élèves, la capacité de confinement et la gestion de nombreux utilisateurs (élèves, professeurs) selon des horaires variés. **Salto** est très populaire dans l'éducation (en particulier les résidences universitaires et les bâtiments académiques de l'enseignement supérieur) en raison de son mélange de serrures hors ligne/en ligne – les universités peuvent installer des serrures Salto sur chaque chambre de dortoir et salle de classe, en utilisant les cartes d'identité étudiantes comme clés, et les gérer de manière centralisée. Le contrôle en temps réel des portes périmétriques avec des serrures sans fil en ligne, ainsi que la capacité hors ligne sur les portes intérieures, offre un bon équilibre entre coût et sécurité. De nombreuses universités ont utilisé Salto pour les résidences tout en utilisant peut-être Software House ou Lenel pour le campus principal – mais Salto peut tout faire avec une planification adéquate. **Dormakaba** possède également une vaste expérience dans l'éducation (leur gamme Keyscan est utilisée sur les campus nord-américains, ainsi que leurs serrures sans fil pour les dortoirs). Pour les écoles primaires et secondaires (K-12), la facilité d'utilisation et la fonction de confinement sont essentielles : **Kisi** ou **Openpath** pourraient être de bons choix pour un district qui souhaite gérer de manière centralisée plusieurs bâtiments scolaires avec une interface simple et délivrer des identifiants mobiles au personnel (et peut-être des badges pour le personnel plus âgé). Kisi commercialise même des cas d'utilisation pour le travail hybride et les gouvernements locaux qui sont parallèles aux besoins des écoles (gestion à distance, intégration facile avec la notification d'urgence) (Source: getkisi.com. Cela dit, le K-12 préfère souvent le sur site pour la fiabilité – **Honeywell ou JCI** conviendraient aux grands districts qui intègrent l'accès avec des systèmes vidéo et de sonorisation pour la réponse d'urgence. **Verkada** a également spécifiquement ciblé les écoles K-12, avec des fonctionnalités comme des boutons de confinement dans leur interface et l'affichage immédiat de la caméra lors d'événements de porte, ce qui est précieux dans les scénarios de menace active. La facilité de distribution de Verkada (gestion cloud sur de nombreux campus) et ses capteurs environnementaux (détection de vape dans les salles de bain) sont des ajouts que les écoles apprécient. Si un district scolaire valorise une sécurité intégrée avec un minimum de charge informatique, **Verkada** est une forte recommandation. Si une université souhaite un contrôle précis et tirer parti des identifiants étudiants existants, **Salto** ou **Dormakaba** sont recommandés, éventuellement couplés à un système d'entreprise pour les laboratoires de recherche de haute sécurité (certains laboratoires pourraient même avoir besoin de **Johnson Controls** pour les zones de sécurité de niveau gouvernemental). Pour les écoles soucieuses des coûts, **Brivo** ou **Kisi** peuvent fournir un contrôle d'accès de base avec des frais récurrents modestes et sont relativement simples, mais pourraient avoir besoin de compléter des éléments comme l'intégration des horaires de cours (une certaine intégration SIS pourrait être possible via des API).

En conclusion, les **10 meilleures solutions excellent chacune dans des niches différentes** :

- **Kisi** – la meilleure solution globale pour les entreprises recherchant un système cloud moderne et facile à intégrer ; excellent pour les PME et les entreprises axées sur la technologie.
- **Johnson Controls (C•CURE)** – le meilleur pour les grandes entreprises/gouvernements nécessitant une sécurité maximale, une intégration et un contrôle sur site.
- **ADT** – idéal pour ceux qui souhaitent un package de sécurité complet avec un minimum de tracas (par exemple, petites entreprises, commerce de détail, franchises) tirant parti du réseau de surveillance et de services d'ADT.
- **ACRE/Feenics** – excellent pour les entreprises qui veulent un logiciel cloud mais sur du matériel ouvert, en maintenant la flexibilité (par exemple, celles qui migrent d'anciens systèmes Lenel ou Software House vers le cloud).
- **Verkada** – parfait pour les organisations multi-sites et les écoles qui valorisent une gestion cloud unifiée de l'accès + des caméras avec une expérience utilisateur extrêmement simple et une forte conformité en matière de sécurité.
- **Brivo** – un pionnier du cloud éprouvé, adapté à un large éventail d'industries (en particulier la gestion multi-propriétés, l'immobilier commercial et le résidentiel multi-familial) où une intégration robuste (par exemple, avec la vidéo, les systèmes de visiteurs) et la fiabilité sont importantes.
- **Avigilon Alta (Openpath)** – un excellent choix pour les bureaux modernes, les immeubles multi-locataires et les campus technologiques qui privilégient un design matériel élégant, la facilité d'utilisation et l'accès mobile-first, désormais soutenu par l'écosystème de Motorola pour des capacités étendues.
- **Dormakaba** – le meilleur lorsque un projet implique de nombreuses portes et des besoins de verrouillage variés (hôtels, grands bureaux, aéroports) et que vous souhaitez un seul fournisseur pour le matériel de porte sophistiqué et le système électronique – c'est la référence pour l'hôtellerie et souvent les grandes infrastructures comme les aéroports ou les métros.
- **Salto** – fortement recommandé pour l'éducation, le co-living/co-working et tout scénario avec de nombreuses portes et utilisateurs dispersés – il offre un mélange hors ligne et en ligne qui peut réduire considérablement les coûts d'installation tout en offrant un contrôle centralisé.
- **Honeywell** – idéal pour les environnements de sécurité complexes et intégrés comme les hôpitaux, les aéroports et les campus industriels qui nécessitent non seulement un contrôle d'accès, mais aussi un lien étroit avec les alarmes, le CVC et les rapports de conformité – la longévité et l'orientation entreprise de Honeywell sont payantes ici.

En alignant les besoins de l'organisation (cloud vs sur site, échelle, intégration, expérience utilisateur, budget) avec les atouts de ces solutions, les consultants en sécurité et les gestionnaires d'installations peuvent sélectionner un système qui non seulement sécurise leurs locaux, mais améliore également l'efficacité opérationnelle et la commodité pour l'utilisateur. L'industrie s'oriente clairement vers des systèmes gérés par le cloud et adaptés aux mobiles, mais les systèmes hérités restent pertinents pour les scénarios très sécurisés et personnalisés. Quel que soit le système choisi, il est crucial de planifier l'évolutivité future, d'assurer une formation adéquate et de collaborer avec des intégrateurs certifiés ou le fournisseur pour un déploiement réussi. Avec l'une de ces 10 meilleures solutions, lorsqu'elles sont correctement mises en œuvre, les organisations seront bien équipées d'une infrastructure de contrôle d'accès sécurisée, agile et moderne pour l'avenir.

Sources : L'analyse et les recommandations ci-dessus font référence à des données et des affirmations issues de la documentation officielle des produits et de sources industrielles crédibles, y compris le rapport 2025 sur le contrôle d'accès de Kisi, le blog de comparaison 2024 de Genea, les classements industriels de 360Connect et Gatewise, et les livres blancs de sécurité des fournisseurs (par exemple, Brivo, Verkada, Salto), entre autres, tels que cités tout au long du document. Ces citations garantissent que les informations sont à jour et soutiennent l'évaluation des fonctionnalités de chaque solution et de leur adéquation à divers cas d'utilisation.

Étiquettes: systemes-controle-acces, securite-physique, gestion-cloud, identifiants-mobiles, conformite-securite, gestion-installations, integration-systemes

---

À propos de 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.
