

# Rapport sur l'état du contrôle d'accès physique en 2024

Un rapport de tendances d'IFSEC Insider

 **IFSEC  
INSIDER**

**HID**



## Avant-propos

Chers lecteurs,

C'est avec une grande fierté que je vous présente notre rapport annuel sur l'état du contrôle d'accès physique pour l'année 2024. En tant que nouvelle Directrice de Marché français pour HID, je vois dans ce rapport une occasion précieuse d'écouter et de comprendre les besoins spécifiques de nos clients, afin de développer des solutions adaptées aux exigences régionales et locales actuelles et futures. Près de deux ans se sont écoulés depuis notre dernier rapport sur l'état du contrôle d'accès physique, et le paysage a considérablement évolué mettant en avant les tendances suivantes :



### Transition vers le télétravail et les modèles hybrides

La pandémie mondiale a accéléré l'adoption du télétravail et des modèles hybrides. En France, le télétravail est passé de 25 % à 36 %, soulignant la nécessité de nouvelles approches en matière de sécurité et de gestion des accès.

### Croissance du marché mondial

Le marché des équipements de contrôle d'accès physique électronique devrait atteindre 9,6 milliards de dollars en 2027. Cette croissance est soutenue par une demande accrue pour des solutions de sécurité sophistiquées et intégrées.

### Adoption rapide de nouvelles technologies notamment sans contact

L'innovation technologique transforme le contrôle d'accès physique, allant au-delà des simples cartes physiques. Les solutions avancées intègrent désormais l'accès mobile, la biométrie et l'authentification multifactorielle pour une sécurité et une efficacité accrue.

### Focus sur l'expérience utilisateur

Les utilisateurs recherchent des solutions sécurisées et faciles à utiliser. L'accent est mis sur la simplification de la gestion des accès et l'amélioration de l'efficacité sans compromettre la sécurité.

### Notre Engagement

Nos solutions de contrôle d'accès reposent sur trois piliers : l'innovation technologique, l'amélioration de l'expérience utilisateur et l'interopérabilité. Ces principes nous guident pour développer des solutions de sécurité avancées, adaptées aux besoins spécifiques de nos clients en France et dans le monde.

Nous croyons en la collaboration et en l'importance de l'expertise pour répondre aux attentes évolutives des utilisateurs. En réimaginant les espaces de travail, nous visons à offrir des expériences utilisateur interactives et intégrées.

Je tiens à exprimer ma gratitude envers tous les participants qui ont contribué à ce rapport. Votre collaboration est précieuse et nous permet de continuer à innover pour mieux vous servir.

Nous espérons que ce rapport vous apportera des informations précieuses et vous aidera à prendre des décisions éclairées pour sécuriser vos environnements physiques et numériques.

Sincères salutations,

**Clara Bardou**  
Directrice de Marché, France, HID

## À propos de HID

HID assure l'identité de confiance des personnes, des lieux et des objets dans le monde entier.

Chaque jour, des millions de personnes utilisent ses produits et services pour accéder de manière sécurisée à des lieux physiques et numériques. La technologie de HID est utilisée pour ouvrir des portes, entrer dans des pays, accéder à des réseaux numériques, vérifier des transactions et suivre des actifs - tout cela grâce à des solutions faciles à gérer telles que les cartes intelligentes, les identifiants mobiles, les passeports ainsi que les lecteurs d'empreintes digitales et la reconnaissance faciale.

La technologie de HID aide les entreprises à identifier, vérifier et suivre de manière sécurisée des milliards d'éléments à l'échelle mondiale. En tout, plus de 2 milliards d'éléments qui doivent être identifiés, vérifiés et suivis sont connectés grâce à la technologie de HID.

Avec ses partenaires, HID est à la pointe du matériel, des logiciels et des services qui permettent aux personnes de naviguer avec confiance dans les mondes physique et numérique.

L'entreprise collabore avec des gouvernements, des universités, des hôpitaux, des institutions financières et certaines des entreprises les plus innovantes au monde - les aidant à créer des environnements physiques et numériques de confiance pour que celles-ci et les personnes qui les utilisent puissent réaliser leur potentiel.

Fondée en 1991, HID a son siège à Austin, Texas. Elle compte plus de 4 500 employés dans le monde et opère des bureaux internationaux soutenant plus de 100 pays. HID est une marque indépendante au sein du groupe ASSA ABLOY.

Pour plus d'informations, visitez [www.hidglobal.com](http://www.hidglobal.com).



## Méthodologie

Le rapport sur l'état du contrôle d'accès physique de 2024 a été réalisé entre novembre 2023 et janvier 2024 et promu par HID et IFSEC Insider.

L'enquête a été distribuée via des partenaires de publication, les médias sociaux et les équipes de vente internes par email.

La diversité des répondants et des secteurs d'activité représentés dans cette enquête offre une vue d'ensemble complète et détaillée des tendances actuelles et des défis du contrôle d'accès physique dans différents contextes géographiques et industriels.

### Collecte des données

Nous avons recueilli 806 réponses à 32 questions, bien que toutes les questions n'aient pas été répondues par tous les participants. Certaines questions permettaient également des réponses multiples, totalisant parfois plus de 100 %.

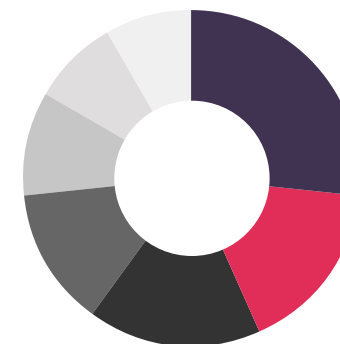
### Répartition géographique

Le sondage couvre plusieurs pays, majoritairement anglophones, avec 93 répondants en France. En tout, 115 pays sont représentés dans les réponses, dont 23 pays européens (hors France).



### Profil des participants

- Directeurs ou responsables de la sécurité : 21 %
- Installateurs, ingénieurs, techniciens et intégrateurs : 19 %
- Consultants et concepteurs de sécurité : 16 %
- Cadres supérieurs : 6 %
- Gestionnaires d'installations : 7 %



### Secteurs d'activité représentés

- Industrie manufacturière : 16 %
- Services professionnels : 10 %
- Gouvernement/Secteur public : 10 %
- Logiciels, technologies, communications : 8 %
- Soins de santé : 6 %
- Vente au détail : 5 %
- Banque : 5 %

« La forte présence européenne dans le rapport de cette année est particulièrement encourageante compte tenu de la nature mondiale de l'enquête. Il y a un marché florissant et croissant du contrôle d'accès en Europe, avec des professionnels de la sécurité dans divers secteurs cherchant activement des solutions innovantes. »

– Gerald Grattoni, Vice-Président et Chef des marchés matures.

# Etat des lieux du marché du contrôle d'accès physique

## Prévalence des technologies traditionnelles et modernes

Pour mieux comprendre l'état actuel du marché du contrôle d'accès physique, nous avons demandé aux personnes interrogées quelles étaient les technologies d'identification qu'elles utilisaient actuellement pour le contrôle d'accès. L'analyse des résultats de notre enquête révèle une coexistence notable entre les technologies traditionnelles et modernes.

Au global, une entreprise sur trois (33 %) utilise encore des cartes de proximité à basse fréquence 125 kHz, et 28 % des entreprises déclarent qu'elles possèdent encore des systèmes compatibles avec la technologie à bande magnétique.

Les technologies telles que la première génération de MIFARE Classic et HID iCLASS® sont toujours utilisées par 19 % et 15 % des organisations respectivement (contre 18 % et 26 % dans notre enquête de 2022). Ces systèmes anciens représentent pourtant un risque de sécurité beaucoup plus élevé. Non seulement les pirates peuvent cloner plus facilement ces technologies non cryptées, mais les systèmes traditionnels ne bénéficient pas des dernières mises à jour de sécurité.

En France, l'adoption de technologie plus récente semble plus rapide. Les entreprises délaissent les technologies traditionnelles comme les cartes de proximité à basse fréquence de 125 kHz et les bandes magnétiques. En effet, seulement 21 % des entreprises utilisent des cartes de proximité à basse fréquence de 125 kHz, et 10 % des solutions à bandes magnétiques.

« Afin de réduire ainsi les risques de sécurité associés aux systèmes traditionnels, nous conseillons aux entreprises de passer à des technologies plus sécurisées telles que Seos ou MIFARE DESFire, qui peuvent être installées très facilement et à moindre coût. »

– Anne Brooks, Directrice Marketing Produit chez HID, Solutions d'Identifiants et Biométriques.



## Seos® et les solutions mobiles en hausse

Seos® – une technologie de contrôle d'accès hautement sécurisée de HID qui utilise l'authentification mutuelle et la cryptographie – est utilisée par 18 % des répondants, sous forme de carte ou mobile. C'est une hausse de 10 % dans notre rapport précédent sur les tendances du Contrôle d'Accès Physique de 2022. D'autres solutions d'accès mobiles sont également citées par 15 % des organisations.

L'une des tendances les plus marquantes est la montée en puissance des technologies biométriques et mobiles. Lorsqu'on leur a demandé s'ils avaient installé, mis à jour ou conseillé sur des projets impliquant des solutions de contrôle d'accès mobile au cours des 12 derniers mois, 65 % des répondants à notre enquête ont répondu par l'affirmative.

Même si leur adoption est encore relativement faible, la présence de solution Mobile, QR Code, et BLE (Bluetooth Low Energy) signale un avenir où les solutions de contrôle d'accès seront de plus en plus intégrées avec les dispositifs mobiles, offrant une plus grande commodité et une meilleure sécurité.

Ces technologies, en permettant l'intégration avec les smartphones et autres dispositifs portables, offrent une flexibilité accrue et un potentiel d'amélioration continue de la sécurité.

## Le badge physique encore répandu

Les technologies d'identification se diversifient avec des solutions comme les QR codes, les systèmes de reconnaissance automatique de plaques d'immatriculation, la biométrie et le suivi de localisation.

Cependant, notre enquête révèle que les badges d'identification physiques restent majoritaires, étant encore utilisés dans 63 % des organisations. Les systèmes de gestion du temps et de présence, permettant aux employés d'enregistrer leurs heures pour des raisons de paie et d'administration, sont également populaires, utilisés dans 60 % des entreprises. De même, les systèmes de contrôle des parkings et des barrières, destinés à surveiller les entrées et sorties des véhicules, sont employés dans 60 % des organisations.

Sans surprise, compte tenu de la transition vers des modes de travail hybrides, deux tiers des organisations (66 %) utilisent désormais activement l'accès logique (connexion sécurisée à un ordinateur/réseau pour accéder aux ressources cloud et web). C'est en hausse par rapport aux 55 % de notre précédente enquête sur les tendances du contrôle d'accès physique en 2022. D'autres technologies établies actuellement déployées et utilisées activement sur le marché incluent la gestion d'impression sécurisée et les applications de ronde de sécurité, toutes deux à 43 %.

Cependant, bien que les badges d'identification physiques restent extrêmement populaires, nous constatons une transition vers de nouvelles technologies d'identification.

**Notre enquête révèle que la technologie biométrique est déployée par une organisation sur trois (31 %), qu'il s'agisse de la reconnaissance d'empreintes digitales, faciale ou de l'iris pour le contrôle d'accès, ou utilisée pour l'authentification à deux facteurs, comme couche de sécurité supplémentaire.**



**Sanjit Bardhan**  
Vice-Président mobile, HID

## Développer l'expérience utilisateur

Par ailleurs, 39 % des entreprises utilisent désormais activement des identités mobiles (contre 32 % dans notre rapport de 2022). L'utilisation d'identifiants mobiles permet aux organisations, en particulier dans le secteur de l'immobilier commercial, d'offrir des fonctionnalités supplémentaires aux utilisateurs, de se différencier et de facturer des loyers plus élevés.

« De plus en plus, nous voyons des entreprises combiner le contrôle d'accès physique avec une expérience plus numérique via le mobile. Par exemple, avec une application, les utilisateurs peuvent réserver des salles de réunion ou payer la nourriture à la cantine. »

– **Sanjit Bardhan, Vice-Président mobile, HID**

Concernant les coûts, M. Bardhan affirme qu'il y a très peu de différence entre l'utilisation de cartes d'identification physiques et l'accès mobile. « Tous les lecteurs que nous avons vendus au cours des trois dernières années prennent en charge l'accès mobile et peuvent être configurés pour la clé mobile spécifique du client. Pour les installateurs, il n'y a pas de travail supplémentaire. »

## Des systèmes qui répondent aux exigences des organisations

92 % des organisations estiment que leurs PACS répondent aux exigences. Ce taux de satisfaction des systèmes de contrôle d'accès physique (PACS) a récemment montré une légère hausse. En 2022, 12 % des répondants ont déclaré que leur PACS actuel ne répondait pas aux exigences organisationnelles. Aujourd'hui, ce chiffre est tombé à 8 %, retrouvant ainsi le niveau de satisfaction de 2020.

Cette fluctuation pourrait indiquer que l'année 2022 était une exception, probablement en raison des perturbations de la chaîne d'approvisionnement liées à la pandémie de Covid, qui ont retardé les mises à niveau des systèmes. En parallèle, un plus grand nombre de répondants affirme maintenant que leur système répond à toutes les exigences actuelles (38 % contre 33 % en 2022), et 7 % estiment même que leur système dépasse les attentes (contre 3 % en 2022).

Notre rapport indique également que la plupart des organisations utilisent des technologies de contrôle d'accès relativement récentes. Il y a une répartition égale entre les systèmes de moins de trois ans et ceux de trois à six ans (31 % chacun). Les systèmes hérités de plus de six ans, qui posent un risque de sécurité plus élevé, représentent une plus petite part du marché (19 %). A noter cependant, 16 % des répondants ne connaissaient pas l'âge exact de leurs systèmes, ce qui pourrait indiquer un pourcentage réel plus élevé.

Les composants du système, tels que les lecteurs, les identifiants et les contrôleurs, sont moins souvent mis à jour. En revanche, les logiciels sont généralement plus récents. En effet, 42 % des répondants ont déclaré que leur logiciel a moins de trois ans, tandis que seulement 14 % ont indiqué qu'il a plus de six ans. Cette tendance est probablement due à la demande croissante pour des solutions de contrôle d'accès en tant que service (ACaaS).

Plus de la moitié des organisations prévoient de mettre à niveau au moins certains composants de leurs systèmes de contrôle d'accès dans les six prochaines années. Plus précisément, 54 % prévoient de mettre à niveau leurs logiciels, 53 % leurs lecteurs et identifiants, et 50 % leurs contrôleurs.

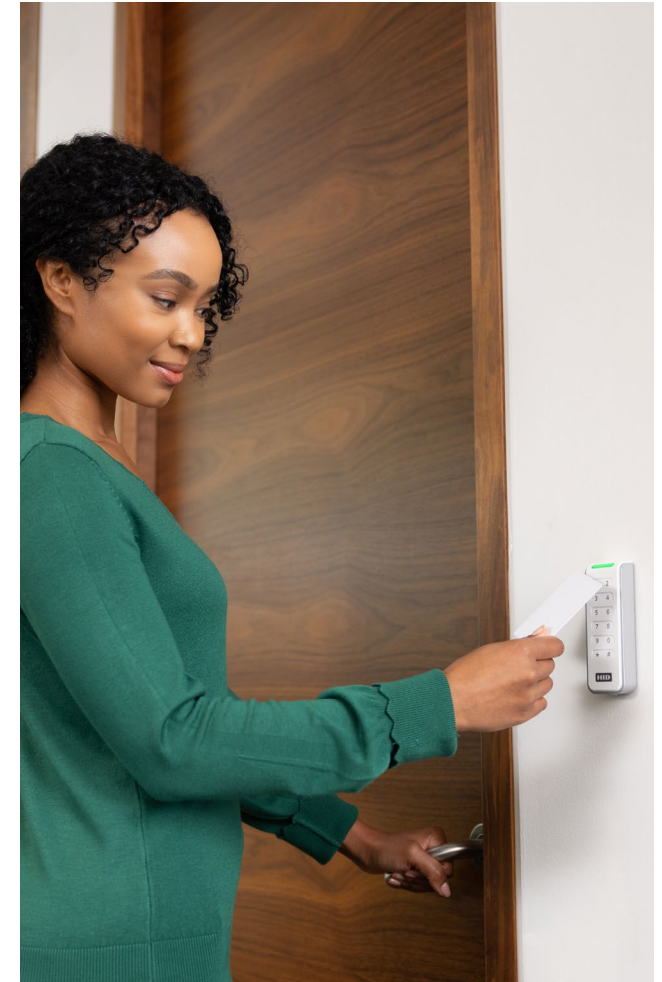
« Nous croyons en une conception durable et évolutive. Même si prédire l'avenir avec précision est impossible, il est possible de se préparer en mettant l'accent sur l'innovation continue et en facilitant la migration vers les nouvelles technologies. Votre solution de contrôle d'accès doit être sécurisée, et permettre d'intégrer facilement des avancées comme la localisation et la biométrie

afin de toujours rester à la pointe de l'innovation en matière de sécurité »

– Cristian Cotiga, Vice-président de la gestion des produits, HID.

### Priorités : simplicité, sécurité, et interopérabilité

Lors de l'installation de systèmes de contrôle d'accès physique, la facilité de la gestion des accès et la protection contre les failles de sécurité sont les défis majeurs pour 50 % des répondants français. Suivi par le respect des nouvelles réglementations pour 46 % d'entre elles. L'amélioration de l'expérience utilisateur arrive en 4<sup>e</sup> position, citée à 32 %. Par ailleurs, 18 % des répondants ont cité l'intégration avec d'autres systèmes d'entreprise comme l'un des trois principaux défis quotidiens. Ce constat souligne l'importance croissante de l'interopérabilité dans le contrôle d'accès physique, comme indiqué dans un eBook publié en 2021 par IFSEC Global<sup>3</sup>. En effet, les résultats de cette étude montrent une forte demande pour des systèmes plus intégrés, avec une transition vers des standards ouverts tels que le protocole OSDP (Open Supervised Device Protocol). Ce standard améliore non seulement l'interopérabilité entre les produits de contrôle d'accès, mais offre également une sécurité accrue grâce au cryptage AES-128 et à une surveillance continue du câblage pour prévenir les falsifications.



<sup>3</sup> [Coup de projecteur sur OSDP, HID Global](#)



## Espaces de travail intelligents : l'impact de la géolocalisation

La gestion du nombre et de l'emplacement des employés et des visiteurs dans un bâtiment est un défi majeur pour l'industrie de la sécurité, accentué par l'essor du travail hybride. En analysant les données d'occupation, les entreprises peuvent ainsi identifier les zones sous-utilisées et prendre des décisions éclairées pour optimiser la conception de leurs espaces de travail.

Cela peut se traduire par des économies d'énergie en réduisant le chauffage et l'éclairage dans les zones inoccupées. Ces données peuvent également guider les décisions sur la conservation, la vente ou la sous-location des bâtiments.

Selon notre enquête, un quart des répondants ont cité la connaissance de la présence et de l'emplacement des personnes dans le bâtiment comme l'un de leurs trois principaux défis. Plus de deux répondants sur cinq (41 %) déclarent qu'ils "connaissent à la fois le nombre et l'emplacement des employés et des visiteurs", tandis qu'un tiers (33 %) "connaissent le nombre d'employés et de visiteurs mais pas leur emplacement". Il est important de noter que toutes ces données sont anonymisées et ne peuvent être liées à un individu.

« Le passage à un modèle de travail hybride a introduit de nouveaux défis en matière de sécurité et de gestion de l'espace. Les solutions d'accès mobile jouent un rôle crucial afin d'exploiter pleinement ce potentiel. Elles permettent aux entreprises de mieux comprendre l'utilisation de leurs espaces, les aidant à créer des lieux de travail plus efficaces et durables. »

– **Katarina Björk, Directrice des services de localisation chez HID.**

Diverses méthodes sont utilisées pour recueillir ces informations, les systèmes de contrôle d'accès et la numérisation des badges étant les plus courantes, adoptées par 48 % des organisations. Parmi les autres solutions de localisation, on trouve les systèmes de temps et de présence (29 %), les registres électroniques (18 %) et même les registres papier (17 %). Moins répandus sont les systèmes de suivi de localisation (14 %) et les systèmes de suivi par SMS ou téléphone mobile (7 %).

## Défis et exigences des mises à niveau des systèmes de contrôle d'accès

Avec l'évolution de la technologie et des logiciels, le contrôle d'accès est de plus en plus intégré à d'autres domaines au sein d'une organisation, notamment les ressources humaines, les installations, les technologies de l'information. Cette évolution a inévitablement affecté le processus d'achat et de prise de décision concernant les mises à niveau des équipements, des composants matériels ou des logiciels utilisés pour le contrôle d'accès.

Les résultats de notre enquête montrent clairement que les installateurs, les intégrateurs, les consultants et les vendeurs qui traitent directement avec l'utilisateur final doivent de plus en plus concilier des demandes et des influences multiples provenant de plusieurs départements lors de la mise à niveau des systèmes. En conclusion, la géolocalisation et l'optimisation des espaces sont cruciales pour améliorer l'efficacité et la durabilité des bâtiments, surtout dans le contexte du travail hybride. Les solutions d'accès mobile jouent un rôle clé en fournissant les données nécessaires pour cette transformation.

## Le choix des systèmes de contrôle d'accès : vers une approche plus collaborative

Bien que l'autorité finale demeure souvent entre les mains des dirigeants exécutifs comme le CISO, le CIO, le CTO, ou le département de sécurité physique, de nombreux autres départements exercent une influence sur le processus décisionnel, y compris l'environnement (38 %), les services généraux (31 %), les achats (28 %) et les IT (21 %).

La collaboration entre les départements de sécurité physique et de sécurité informatique devient essentielle. Près de la moitié (48 %) des répondants ont indiqué que le département informatique est « pleinement consulté » pour les mises à niveau des systèmes de contrôle d'accès physique, malgré une influence globale moins importante que d'autres départements.

De plus, 53 % des participants ont affirmé que le département informatique joue régulièrement un rôle décisif ou influe dans les décisions de mise à niveau, se situant derrière le département de sécurité physique (71 %), mais devant les services généraux (50 %), la sécurité informatique (35 %), les achats (27 %) et les cadres supérieurs (24 %).

« La transition vers l'accès mobiles nécessite un écosystème de partenaires, du fabricant des systèmes d'accès mobile aux intégrateurs qui installent les lecteurs et intègrent les différentes plateformes logicielles et matérielles dans votre installation. L'expérience, les références de sécurité vérifiées et un large portefeuille de solutions sont essentiels pour un déploiement réussi. Que vous soyez une entreprise régionale ou une grande université, vous avez besoin de partenaires qui comprennent vos besoins, offrent des solutions centrées sur le client et rendent la transition aussi fluide et économique que possible. »

– Sanjit Bardhan, Vice-Président, Mobile chez HID.

## Synergie entre sécurité physique et informatique

Concernant la collaboration avec le département informatique, 58 % des répondants ont mentionné la mise en place de bonnes pratiques de sécurité pour leurs installations, et 55 % recherchent ensemble de nouvelles technologies. Seuls 24 % ont indiqué qu'il y avait « peu ou pas de chevauchement » entre les deux départements.

Cette évolution n'est pas surprenante. De nombreux experts estiment que les organisations doivent fusionner leurs opérations de sécurité physique et informatique.

À mesure que les systèmes de sécurité physique évoluent vers des produits basés sur IP, ils sont désormais directement connectés au réseau informatique de l'organisation. Les professionnels de l'informatique doivent s'assurer que tout ce qui est attaché à leur réseau respecte les normes telles que l'ISO 27001 – une norme mondialement reconnue pour la gestion de la sécurité de l'information – et évaluer les risques liés aux hackers via les vulnérabilités présentes dans, par exemple, une unité de contrôle d'accès.



## 5 Tendances technologiques dans le contrôle d'accès physique

### 1. Accès mobile et identités numériques destinés à devenir omniprésents

Bien que les identifiants physiques soient encore très présents dans l'industrie du contrôle d'accès, il ne fait aucun doute que les identifiants mobiles et les identités numériques gagnent rapidement du terrain. Selon ce rapport, près de 2 personnes sur 5 (39 %) utilisent désormais activement des identités mobiles, les solutions sans contact (48 %) et l'accès mobile (44 %) étant les deux principales tendances façonnant l'industrie du contrôle d'accès.

Omdia estime que près de 50 millions d'identifiants mobiles ont été téléchargés dans le monde en 2022 et que les revenus des ventes d'identifiants mobiles croîtront à un taux de croissance annuel composé (CAGR) de 39,8 % de 2022 à 2027<sup>4</sup>.

Dans le dernier rapport HID 2024 sur l'état de la sécurité et de l'identité, les professionnels de la sécurité interrogés déclarent que près de 80 % des organisations déploieront des ID mobiles dans les cinq prochaines années, tandis que les partenaires de l'industrie sont

encore plus optimistes, affirmant que 94 % de leurs clients auront déployé des ID mobiles d'ici 2029.

#### Les identifiants mobiles : une solution pratique et moderne pour le contrôle d'accès

Les identifiants mobiles sont plébiscités pour leur facilité d'utilisation. En permettant aux utilisateurs de sauvegarder leurs identifiants directement sur leur téléphone, ils offrent une alternative attrayante aux systèmes traditionnels. Une solution qui séduit d'ailleurs de plus en plus d'organisations puisque 62,5 % des répondants françaises ont indiqué avoir installé des solutions de contrôle d'accès mobile au cours des 12 derniers mois, tandis que ce chiffre atteint 70,4 % à l'échelle mondiale.

Les identifiants dans des portefeuilles numériques tels qu'Apple Wallet ou Google Wallet™ permettent aux utilisateurs de smartphones et de montres connectées d'accéder à des bâtiments, de se connecter à leur poste de travail et même d'imprimer des documents, sans nécessiter de carte physique. Cette technologie est notamment de plus en plus utilisée pour les cartes d'identité des étudiants et des clients d'hôtels.

<sup>4</sup> [IFSEC Global, Tendances, opportunités et défis en matière de contrôle d'accès physique](#)



**Stephenie Haldane**  
Vice-Présidente du développement  
commercial, HID

Les avantages des identifiants mobiles incluent :

- **Praticité** : Plus besoin de transporter plusieurs cartes physiques.
- **Sécurité** : Les identifiants numériques bénéficient des mesures de sécurité des smartphones.
- **Polyvalence** : Utilisation possible pour divers accès et services au sein de l'entreprise.

« En adoptant cette technologie, les entreprises peuvent non seulement améliorer l'efficacité et la sécurité de leurs systèmes de contrôle d'accès, mais aussi offrir une expérience utilisateur fluide et moderne. »

– **Stephenie Haldane, Vice-Présidente du développement commercial, HID.**

## 2. Les normes ouvertes : pilier de l'essor des bâtiments intelligents

Les normes ouvertes ont longtemps été évoquées dans le domaine du contrôle d'accès, mais ce n'est que récemment que leurs avantages ont vraiment émergé. Prenons l'exemple du protocole OSDP : bien qu'il ait été développé en 2008, il n'est devenu une norme de la Commission Électrotechnique Internationale (CEI) qu'en 2020. Depuis, il a fortement contribué à l'essor des bâtiments intelligents.

Selon Fortune Business Insights<sup>5</sup>, le marché mondial des bâtiments intelligents passera de 96,96 milliards de dollars en 2023 à 408,21 milliards de dollars d'ici 2030, avec un taux de croissance annuel composé (CAGR) de 22,8 %. Cette tendance se reflète dans notre enquête, où 43 % des répondants placent « les bâtiments intelligents et les espaces de travail flexibles » parmi les trois principales tendances du contrôle d'accès, juste derrière les solutions sans contact (48 %) et l'accès mobile/applications mobiles (44 %). De plus, près d'un tiers (32 %) des répondants ont mentionné l'intégration avec d'autres fonctions de l'entreprise, comme les ressources humaines, la CVC (chauffage, ventilation et climatisation), l'éclairage et la réservation de bureaux, comme une tendance clé.



Les normes ouvertes encouragent des solutions de sécurité plus intégrées, où les données de contrôle d'accès servent non seulement à réguler l'accès, mais aussi à optimiser l'utilisation des espaces. Avec l'augmentation du travail hybride, il est essentiel pour les entreprises de s'appuyer sur les données d'occupation pour affiner leur stratégie et réduire les coûts.

L'utilisation des identifiants mobiles pour le contrôle d'accès permet notamment de déterminer quelles parties du bâtiment sont utilisées à quels moments, assurant ainsi que seules ces zones soient chauffées, éclairées et alimentées en électricité. Près de la moitié (48 %) des organisations utilisent déjà des systèmes de contrôle d'accès/scan de badges pour surveiller l'utilisation du bâtiment tout au long de la journée.

Cependant, cette approche intégrée présente des défis. L'intégration accrue des systèmes de contrôle d'accès physique dans les bâtiments intelligents offre de nouvelles opportunités aux cybercriminels pour attaquer l'infrastructure des entreprises. Il est donc essentiel que les systèmes physiques soient gérés en étroite collaboration avec les technologies de l'information (IT).

« La sécurité physique et la cybersécurité sont intrinsèquement liées, et il n'est pas plus efficace de gérer ces menaces séparément. Les incidents cyber-physiques peuvent rapidement entraîner des dommages physiques, des destructions de biens, des catastrophes environnementales et pire encore. »

– Thomas Kopecky, Co-fondateur, Dark Reading<sup>6</sup>.

### 3. L'environnement : une influence croissante sur les décisions commerciales

Autrefois, les professionnels de la sécurité se concentraient uniquement sur l'atténuation des risques. Désormais, les considérations de durabilité jouent un rôle de plus en plus important dans leurs opérations. Notre enquête montre que l'environnement est un facteur significatif dans le contrôle d'accès, avec près de deux tiers (63 %) des répondants affirmant que les responsables de la durabilité sont consultés ou influencent les décisions de mise à niveau des systèmes de contrôle d'accès physique.



<sup>6</sup> [Converging physical and cyber security, iStart Technology in Business](#)



Lorsqu'on leur a demandé quels étaient les principaux moteurs de la mise à niveau de leurs solutions de contrôle d'accès physique, 15 % des participants ont répondu « pour soutenir les objectifs de durabilité de l'entreprise », et 12 % ont mentionné des caractéristiques telles que « le matériel à faible consommation d'énergie » (en légère hausse par rapport à 11 % en 2022).

Les solutions économes en énergie ont également été citées parmi les trois principales tendances façonnant l'industrie du contrôle d'accès à l'avenir par 14 % des répondants, bien que d'autres tendances comme l'accès mobile/sans contact, l'hébergement cloud et la technologie des bâtiments intelligents aient obtenu des scores plus élevés.

Il n'est guère surprenant que la durabilité devienne un facteur clé dans les décisions commerciales. En France, la réglementation a été renforcée et oblige les grandes entreprises à reporter leurs actions en matière de responsabilité sociale. Dans un rapport, KPMG<sup>7</sup>, recense que 95 % des entreprises françaises s'impliquent dans le reporting en matière de développement durable et d'ESG et 75 % disposent d'un Responsable dédié aux questions d'ESG au sein des instances dirigeantes.

Selon le rapport 2024 sur l'état de la sécurité et de l'industrie de HID<sup>8</sup>, les utilisateurs finaux demandent une plus grande transparence sur leur empreinte environnementale, leurs pratiques d'approvisionnement et leurs activités de recherche et développement.

En fait, 87 % des répondants affirment que la durabilité est « importante à extrêmement importante » pour leurs clients, et 76 % ont constaté une augmentation de l'importance de la durabilité pour leurs clients.

Un domaine où les organisations peuvent clairement améliorer leur impact environnemental est la réduction de l'utilisation de plastique.

« Même si les badges physiques offrent une solution d'identification simple, il est essentiel de se tourner vers des alternatives durables et de réduire l'utilisation du plastique. Les badges virtuels sont plus respectueux de l'environnement, génèrent moins de CO2 et aident les entreprises à atteindre leurs objectifs environnementaux. »

– **Steven Commander, Directeur de la réglementation et des relations avec les consultants, HID.**



<sup>7</sup> [Gérer les menaces de sécurité cyber-physique grâce à la convergence dans un monde hyper-connecté](#)

<sup>8</sup> [Le rôle central du contrôle d'accès dans la transition vers les bâtiments intelligents, IFSEC Insider](#)

#### 4. L'essor de l'intelligence artificielle pour les cas d'utilisation analytique

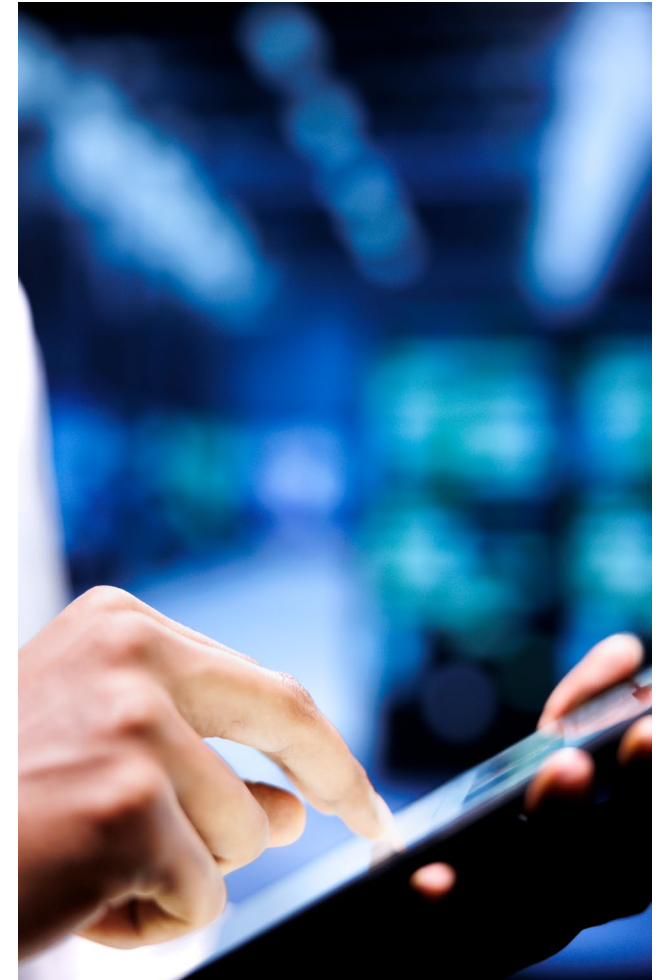
À l'instar d'autres domaines comme la vidéosurveillance, l'utilisation des capacités de l'intelligence artificielle (IA) dans le contrôle d'accès physique devient de plus en plus courante à mesure que les technologies et l'expertise en IA progressent.

Interrogés sur leur intention d'incorporer l'IA ou le machine learning dans leurs solutions de contrôle d'accès, 38 % des répondants à notre enquête ont déclaré qu'ils envisageaient cette possibilité, bien que le même pourcentage ait exprimé des doutes quant aux bénéfices. Seuls 23 % ont affirmé ne pas avoir de plans pour intégrer ces technologies.

Le rapport HID sur l'état de la sécurité et de l'identité révèle que de nombreux professionnels de la sécurité considèrent les capacités analytiques de l'IA comme une opportunité. Plutôt que de s'appuyer sur l'IA pour l'ensemble du système de sécurité, ils voient l'analyse comme un moyen d'opérationnaliser l'IA pour obtenir des résultats immédiats. Dans ce cadre, 35 % des utilisateurs finaux prévoient de tester ou de mettre en œuvre une capacité d'IA dans les trois à cinq prochaines années, tandis que 15 % utilisent déjà des biométries activées par l'IA.

« Par exemple, dans la surveillance avancée des conditions, l'IA et l'apprentissage automatique peuvent être utilisés pour comprendre le comportement normal d'un actif. Lorsque ce comportement change, le système peut déclencher des alertes concernant la température, la puissance, le mouvement, etc. Avec le soutien de l'IA, le système peut également effectuer une maintenance prédictive et des diagnostics. »

« En fin de compte, les capacités de l'IA permettent aux organisations de détecter les menaces plus rapidement, d'obtenir des rapports détaillés et d'analyser de vastes quantités de données plus efficacement, les aidant ainsi à mieux gérer et anticiper les risques. »





## 5. Les solutions biométriques gagnent du terrain

Le marché des biométries est en pleine expansion. D'ici 2031, il devrait atteindre 136,18 milliards de dollars<sup>9</sup>, tandis que la reconnaissance faciale passera de 3,83 milliards de dollars en 2020 à 16,74 milliards de dollars en 2030, avec un taux de croissance annuel composé (CAGR) de 16 % entre 2021 et 2030<sup>10</sup>.

Les technologies biométriques suscitent un vif intérêt dans le domaine du contrôle d'accès. Près d'un quart des répondants (23 %) à notre enquête 2024 ont cité les biométries comme une des principales tendances à surveiller.

Selon le rapport HID 2023 sur l'état de la sécurité, 26 % des répondants utilisent déjà des biométries, avec ou sans contact, et 33 % prévoient d'adopter ces technologies dans les cinq prochaines années.

Alors, quelles technologies les entreprises adoptent-elles et quelles sont les différences régionales ? Ann Brookes et Cristian Cotiga de HID expliquent que les lecteurs d'empreintes digitales restent populaires en Amérique du Nord et en Europe. Cependant, dans les marchés émergents comme l'Afrique, certaines parties de l'Asie et l'Amérique latine, où la reconnaissance des empreintes digitales est déjà courante, les entreprises se tournent de plus en plus vers la reconnaissance faciale.

La reconnaissance faciale offre un avantage majeur : elle est sans contact, un atout particulièrement apprécié durant la pandémie de Covid-19. D'autres technologies sans contact gagnent également en popularité, comme les lecteurs de paume, les lecteurs d'empreintes digitales sans contact et les scanners d'iris.

Omdia prévoit un taux de croissance de 20 %<sup>11</sup> pour la reconnaissance faciale, soutenu par la baisse des prix et la diminution des taux d'erreur des lecteurs avancés. Des études, comme le Face Recognition Vendor Test du NIST, montrent que les algorithmes modernes de reconnaissance faciale peuvent atteindre une précision de 99,97 %<sup>12</sup>. Cependant, peu de fabricants offrent des solutions précises dans des conditions d'éclairage difficiles ou avec des positions de visage non frontales.

<sup>9</sup> [Étude de marché sur la transparence, taille du marché de la biométrie](#)

<sup>10</sup> [Recherche de marché allié, marché de la reconnaissance faciale](#)

<sup>11</sup> [Base de données de contrôle d'accès Omdia](#)

<sup>12</sup> [Informations sur les entreprises Fortune](#)