SÉCURITÉ ENTRÉE

RAPPORT DE TENDANCE

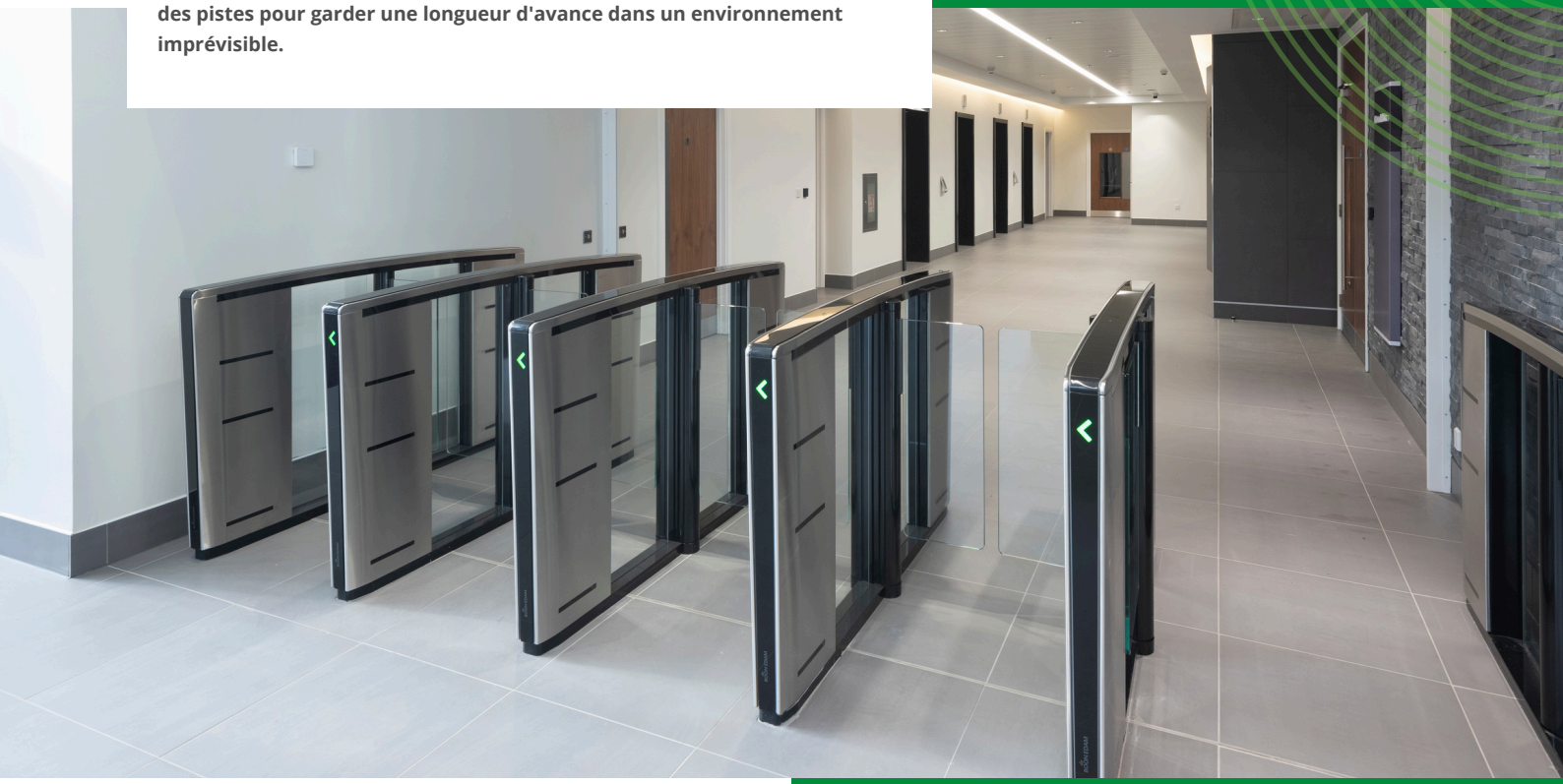
2025.

FAÇONNER **LES ENTRÉES SÉCURISÉES** DE DEMAIN.

BOON EDAM
YOUR **ENTRY** EXPERTS.

INTRODUCTION.

Les exigences en matière de sécurité des bâtiments ont considérablement augmenté dans un monde marqué par une polarisation croissante, des avancées technologiques, un extrémisme et une méfiance grandissante. Les secteurs qui ne nécessitaient autrefois qu'une protection modérée sont désormais confrontés à des risques accrus, les menaces s'étendant au-delà des bâtiments gouvernementaux et des centres de données. Ce rapport explore les tendances actuelles en matière de sécurité des entrées et fournit des pistes pour garder une longueur d'avance dans un environnement imprévisible.



« Alors que la société envisage des environnements sans obstacles et accueillants, la dure réalité exige des mesures de sécurité robustes qui équilibrent l'accessibilité et la protection. »

Douwe Jolles
PRODUCTMANAGER - DOOR SYSTEMS

INDICE

1 CYBER-SÉCURITÉ RENCONTRE SÉCURITÉ PHYSIQUE.

La nécessité d'une approche unifiée de la sécurité n'a jamais été aussi cruciale. Cette intégration ouvre la voie à une nouvelle ère de stratégies de protection pour les organisations de tous secteurs, notamment les centres de données, les bâtiments gouvernementaux, les infrastructures critiques et les sièges sociaux. Dans notre monde connecté, la sécurité ne se limite pas au blocage des accès non autorisés ou à la protection des systèmes numériques : il s'agit de combiner harmonieusement ces deux éléments au sein d'une défense complète et unifiée.

Architecture Zero Trust

Ce modèle de sécurité repose sur le principe du moindre privilège. Il garantit que les utilisateurs et les appareils n'accèdent qu'aux ressources spécifiques requises par leurs rôles, sans plus. Zero Trust rend considérablement plus difficile pour les acteurs malveillants de pénétrer les systèmes ou de voler des informations sensibles en limitant les points d'accès. Cette approche est particulièrement cruciale dans les environnements à enjeux élevés comme les centres de données, où toute faille de sécurité peut avoir de graves conséquences. Dans ce contexte, chaque interaction avec les ressources physiques et numériques doit être vérifiée par rapport aux autorisations d'accès autorisées.

Relever la barre en matière de cybersécurité

De nouvelles réglementations européennes redéfinissent les normes de cybersécurité, impactant directement les entrées sécurisées et les systèmes de contrôle d'accès. La directive NIS2 et le Cyber Resilience Act (CRA) visent tous deux à renforcer la cyberprotection, mais se concentrent sur des aspects différents.

La norme NIS2 vise à sécuriser les services essentiels et les infrastructures critiques. Elle oblige les secteurs comme l'énergie, la santé et les transports à mettre en œuvre des mesures de cybersécurité renforcées. Celles-ci incluent une meilleure gestion des risques, la sécurité de la chaîne d'approvisionnement et un signalement plus strict des cyberincidents. Les organisations qui ne se conformeraient pas à cette norme d'ici fin 2024 s'exposeraient à de lourdes sanctions et à une atteinte à leur réputation.

La loi sur la **cyberrésilience garantit** que les produits dotés de composants numériques, tels que les systèmes de contrôle d'accès, Les portes de sécurité, les couloirs rapides et les portes tournantes IoT intégrant des intégrations numériques doivent respecter des normes de cybersécurité plus strictes. Les fabricants doivent intégrer la sécurité dès la conception, la maintenance et les mises à jour régulières de leurs produits. Certains produits à haut risque nécessitent une certification par un organisme tiers avant leur mise sur le marché européen. Les produits conformes à ces normes porteront le marquage CE, ce qui permettra aux entreprises d'identifier plus facilement les solutions conformes.

Ensemble, ces réglementations établissent une nouvelle référence en matière de cybersécurité, garantissant que l'infrastructure et les produits physiques utilisés pour la sécuriser sont résilients face aux cybermenaces.

Construire des écosystèmes de sécurité

Dans le contexte sécuritaire complexe d'aujourd'hui, l'écosystème de sécurité d'un bâtiment doit intégrer des mesures de sécurité élevées, moyennes et faibles afin de créer une défense dynamique et interconnectée. Chaque niveau de sécurité a une fonction unique : assurer la sécurité du bâtiment, protéger les actifs et garantir l'accès si nécessaire.

Si la cybersécurité domine souvent les discussions sur la protection des environnements sensibles, la sécurité physique est tout aussi cruciale, notamment pour les installations comme les centres de données. Si une personne malveillante accède directement à un serveur, elle peut contourner les pare-feu les plus sophistiqués, ce qui peut entraîner des violations de données catastrophiques. Cela souligne l'importance d'harmoniser les systèmes de sécurité physique et numérique.

Les zones de haute sécurité, telles que les salles de serveurs, nécessitent des solutions de sécurité physique robustes, incluant l'authentification biométrique, des protocoles de communication chiffrés et des solutions d'entrée automatisées et sans surveillance. Ces mesures de protection empêchent les entrées non autorisées et s'alignent sur les stratégies de cybersécurité en permettant des modifications rapides des autorisations afin d'atténuer les menaces en temps réel.

Les zones de sécurité moyenne, comme les étages administratifs, s'appuient sur des technologies telles que les couloirs rapides équipés de capteurs avancés, garantissant un accès fluide au personnel autorisé tout en dissuadant les tentatives d'intrusion. Les espaces de faible sécurité, comme les halls d'entrée publics, privilégient l'esthétique et l'accessibilité tout en maintenant une sécurité essentielle grâce à des points d'accès surveillés.

Cette approche écosystémique reflète les principes de cybersécurité tels que l'authentification multifacteur. Tout comme les systèmes numériques nécessitent des défenses multicouches pour protéger les informations sensibles, les espaces physiques bénéficient de multiples mesures de sécurité complémentaires. Chaque couche garantit qu'en cas de défaillance d'une ligne de défense, les autres restent actives pour protéger les actifs critiques.

Pour garantir l'efficacité de la sécurité physique, il est essentiel d'intégrer les meilleures pratiques de cybersécurité. Cela comprend la mise en œuvre de protocoles de communication chiffrés, la réalisation de mises à jour logicielles régulières et l'utilisation de systèmes de contrôle d'accès résilients contre les cyberattaques.

En concevant un écosystème de sécurité où les mesures de sécurité numériques et physiques fonctionnent en parfaite harmonie, les organisations peuvent créer des espaces sécurisés, opérationnels et préparés aux défis modernes. Cette approche offre non seulement une protection robuste, mais aussi un équilibre entre accessibilité et sécurité, créant ainsi des environnements accueillants et résilients.

Maintenir les intrus à leur place – à l'extérieur – constitue la première ligne de défense. Si un intrus franchit les points d'entrée d'un bâtiment, toutes les autres mesures de sécurité deviennent réactives. Combler la faille de sécurité commence dès l'entrée.

Centre des opérations de sécurité

Un centre d'opérations de sécurité (SOC) est une unité centralisée chargée de la surveillance, de la détection, de l'analyse et de la réponse en temps réel aux menaces de cybersécurité. Son objectif principal est de maintenir la sécurité d'une organisation en protégeant les réseaux, les systèmes, les applications et les données sensibles contre les cybermenaces.

Le SOC fonctionne 24h/24 et 7j/7 pour assurer une surveillance continue et minimiser les risques de violation de données, de cyberattaques ou d'accès non autorisés. Les organisations structurent leurs SOC en fonction de leurs besoins et de leurs ressources spécifiques. Les SOC les plus courants sont les SOC internes, qui offrent un contrôle total des opérations de sécurité, mais nécessitent des investissements importants en personnel et en technologie. Les SOC gérés (ou SOC externalisés) sont exploités par des prestataires de services tiers dotés d'une expertise spécialisée.

2 RÉSISTANCE AUX EXPLOSIONS ET AUX CHOCS.

L'évolution du paysage de la sécurité entraîne une demande croissante de protection renforcée des bâtiments dans un plus large éventail de secteurs. Si les secteurs traditionnels de haute sécurité, tels que les administrations publiques, les banques et les centres de données, ont depuis longtemps privilégié la sécurité, de nouvelles menaces incitent d'autres secteurs, notamment les médias et les entreprises, à renforcer leurs mesures de protection.

Les risques croissants tels que le vandalisme, le terrorisme, les groupes extrémistes et la polarisation sociétale remodèlent l'approche de la sécurité des bâtiments, les matériaux résistants aux explosions et aux chocs devenant des composants essentiels des solutions modernes.

Innovation matérielle

Alors que les entreprises accordent une importance croissante à la prévention des menaces, les entrées résistantes aux explosions et aux chocs deviennent une priorité. L'utilisation croissante de matériaux de pointe pour les façades de bâtiments souligne la nécessité de barrières plus solides pour faire face à l'évolution des risques de sécurité.

Des matériaux tels que les couches de polycarbonate, appréciées pour leur légèreté et leur résistance aux chocs, l'acier renforcé et le verre incassable, sont de plus en plus utilisés dans les systèmes de sécurité modernes. Conçus pour absorber et disperser l'énergie des explosions ou des projectiles, ces matériaux créent des barrières durables qui minimisent les dommages et protègent les occupants. En collaborant avec des experts en science des matériaux, les fabricants intègrent des technologies de pointe à leurs solutions d'entrée, renforçant ainsi leur résistance aux attaques intentionnelles et aux impacts accidentels.

Les entrées sécurisées sont également conçues pour résister aux intrusions violentes, qu'elles soient provoquées par des outils ou des véhicules. Des éléments anti-bélier, des cadres renforcés et des systèmes d'ancrage avancés offrent une protection robuste et constituent une première ligne de défense.

De plus, le verre pare-balles gagne du terrain dans des secteurs auparavant considérés comme à faible risque. Conçu pour absorber et dissiper l'énergie des impacts à grande vitesse, il offre une protection essentielle contre le vandalisme, les incendies criminels et les attaques violentes.

Conséquences économiques des temps d'arrêt

L'impact financier des perturbations causées par des explosions ou des effractions peut être dévastateur, allant souvent au-delà des dommages matériels immédiats. Les interruptions d'exploitation, les pertes d'actifs et l'atteinte à la réputation peuvent impacter les entreprises, en particulier dans les secteurs où les temps d'arrêt affectent directement la confiance des clients et le chiffre d'affaires. Les organisations privilégient de plus en plus la robustesse des entrées comme élément clé de leur stratégie de sécurité, reconnaissant le rôle crucial de ces solutions pour garantir la continuité des activités.

Équilibrer l'accessibilité et la sécurité

Alors que la société privilégie de plus en plus l'ouverture et l'accessibilité, un équilibre délicat doit être trouvé entre la promotion d'écosystèmes immobiliers accueillants et la réponse aux menaces sécuritaires urgentes. Cet équilibre nécessite des solutions innovantes intégrant des fonctionnalités de sécurité avancées sans compromettre l'ouverture et l'esthétique des espaces. Les organisations doivent concevoir des bâtiments non seulement sûrs et résilients, mais aussi en phase avec les valeurs sociétales plus larges, en veillant à ce qu'ils coexistent avec la nécessité de protéger les personnes et les biens dans un monde de plus en plus imprévisible.

3 IA.

L'intelligence artificielle (IA) demeure une priorité majeure dans le secteur des entrées sécurisées. Bien qu'elle puisse parfois paraître surfaite, son potentiel de transformation ne cesse de croître, transformant fondamentalement la manière dont la sécurité est abordée et mise en œuvre.

Les applications pratiques de l'IA, telles que l'analyse prédictive, la détection des menaces et l'automatisation des processus chronophages, sont inestimables. Sa capacité à traiter et interpréter d'importants volumes de données en fait un outil idéal pour la gestion d'environnements complexes tels que les aéroports, les hôpitaux et les entreprises. Dans ces environnements, où les méthodes de sécurité traditionnelles sont souvent insuffisantes, l'IA offre les informations avancées et l'efficacité nécessaires pour garantir la sûreté et la sécurité à grande échelle.

Analyse prédictive et détection des menaces

L'une des applications les plus percutantes de l'IA en sécurité réside dans l'analyse prédictive et la détection des menaces. Les systèmes de sécurité traditionnels reposent souvent sur des mesures réactives, réagissant aux incidents uniquement après leur survenue. L'IA modifie cette dynamique en permettant une approche proactive. En analysant les données de contrôle d'accès et autres données de sécurité en temps réel, les systèmes pilotés par l'IA peuvent détecter les tendances et les irrégularités susceptibles de signaler une menace potentielle.

Au lieu d'attendre que les opérateurs humains détectent ces signaux d'alerte, les systèmes d'IA les signalent automatiquement, hiérarchisent le niveau de risque et fournissent des informations exploitables. Cela garantit des délais de réponse plus rapides et permet aux équipes de sécurité d'intervenir avant que la situation ne dégénère.

SAVIEZ-VOUS?

Le marché mondial de l'IA dans la cybersécurité devrait passer de 25,35 milliards USD en 2024 à 60,24 milliards USD en 2029, à un taux de croissance annuel composé (TCAC) de 19,02 %*.

*Mordor Intelligence. (2024). Rapport sur le marché de l'intelligence artificielle dans la sécurité. Consulté sur https://www.mordorintelligence.com/industry-reports/artificial-intelligence-in-security-market

Innovations basées sur l'IA dans les systèmes d'entrée

L'intégration de l'IA dans les solutions d'entrée telles que les portes tournantes et les couloirs rapides a inauguré une nouvelle ère de sécurité intelligente. L'IA peut prédire les heures de pointe, adapter dynamiquement les fonctionnalités et garantir un débit efficace sans compromettre la sécurité. Ces capacités améliorent à la fois la sécurité et le confort, offrant une expérience utilisateur supérieure tout en répondant aux exigences opérationnelles.

L'authentification biométrique a également atteint de nouveaux sommets. Au-delà de la traditionnelle reconnaissance d'empreintes digitales ou faciale, des méthodes avancées comme l'analyse du réseau veineux et la reconnaissance des pulsations cardiaques sont intégrées aux entrées haute sécurité. Ces innovations renforcent le contrôle d'accès aux zones sensibles tout en assurant une fluidité des flux pour le personnel autorisé.

Innovation durable

Les systèmes d'apprentissage automatique nécessitent d'importantes ressources de calcul ; leur consommation énergétique et leur empreinte carbone doivent donc être gérées avec soin. Le développement de modèles économes en énergie, l'optimisation des infrastructures et l'exploitation des énergies renouvelables sont des étapes essentielles pour réduire l'empreinte environnementale des technologies d'IA. En priorisant ces mesures, les organisations peuvent s'assurer que les progrès de l'IA soutiennent à la fois le progrès technologique et la protection de l'environnement.

Application éthique

Les modèles d'apprentissage automatique doivent être conçus et mis en œuvre sans biais. Les biais en IA peuvent entraîner des résultats discriminatoires, perpétuer les inégalités et saper la confiance dans la technologie. Pour atténuer ce problème, les organisations doivent privilégier des ensembles de données diversifiés et représentatifs, des algorithmes transparents et une évaluation continue. Parallèlement, il est crucial de trouver un équilibre entre sécurité et respect de la vie privée, en veillant à ce que la recherche de la sécurité ne compromette ni les droits individuels ni la vie privée.

L'élément humain : améliorer les décisions grâce à l'IA

Si l'IA offre un potentiel immense, l'humain reste essentiel à l'efficacité des solutions de sécurité. Des décisions plus judicieuses sont prises lorsque les connaissances issues de l'apprentissage automatique sont associées au jugement humain. L'alliance entre l'IA et l'expertise humaine crée un système robuste, capable de relever des défis de sécurité complexes. Cependant, une certaine hésitation persiste à s'appuyer entièrement sur l'IA pour prendre des décisions sans supervision humaine.

En fin de compte, l'IA ne vise pas à remplacer l'humain, mais à lui donner les moyens d'accomplir davantage. En automatisant les tâches routinières, en améliorant la détection des menaces et les capacités de réponse, l'IA permet aux équipes de sécurité de se concentrer sur leur mission principale : protéger les personnes, les biens et les environnements. Malgré ses nombreux avantages, l'IA ne remplace pas l'expertise humaine. Les professionnels de la sécurité apportent un esprit critique, une intuition et une compréhension contextuelle que l'IA ne peut reproduire. Les stratégies de sécurité les plus efficaces reposent sur cette collaboration homme-IA, où l'IA gère la lourde tâche d'analyse et d'automatisation des données, tandis que les humains interprètent les informations et prennent des décisions éclairées.

4 DURABILITÉ.

La demande de solutions durables et respectueuses de l'environnement devient une préoccupation croissante dans le secteur de la sécurité, les organisations cherchant à intégrer la responsabilité environnementale. Si la sécurité reste la priorité absolue, on constate une reconnaissance croissante.

Le développement durable joue un rôle dans les stratégies commerciales à long terme. De plus en plus d'entreprises recherchent des solutions conciliant performances de sécurité, efficacité énergétique et impact environnemental, témoignant d'une évolution vers une approche plus responsable de leurs opérations.

La véritable durabilité ne se limite pas au recyclage ou à la réutilisation ; elle commence par la conception de produits si fiables que ces étapes deviennent secondaires.

Amine Bouchareb
PRODUCTMANAGER - ACCÈS SÉCURITÉ

En 2024, le marché mondial des matériaux de construction écologiques était évalué à environ 369,67 milliards de euro.

Il est prévu qu'il atteigne €1.050,09 milliards de dollars d'ici 2032, avec un taux de croissance annuel composé (TCAC) de 12,3 %.

Rénovation des entrées de sécurité

La rénovation offre une solution économique et durable pour moderniser les entrées sécurisées, améliorant ainsi la protection et l'efficacité sans nécessiter de remplacement complet. En modernisant le contrôle d'accès et en améliorant la sécurité, les entreprises peuvent prolonger la durée de vie des entrées existantes tout en réduisant les déchets et les perturbations. Il existe deux principaux types de rénovations, chacun répondant à des besoins de sécurité et d'exploitation différents :

- **La modification améliore les fonctionnalités,** les performances ou les caractéristiques d'un produit existant sans en altérer l'identité fondamentale. Par exemple, la modification d'une porte d'entrée peut inclure le remplacement de capteurs, le réglage fin de la sécurité ou la modification du contrôle d'accès, permettant ainsi aux organisations de s'adapter aux nouvelles exigences tout en conservant leurs installations actuelles.

- **Une mise à niveau** implique des modifications importantes des performances, des matériaux ou des caractéristiques d'un produit, entraînant une nouvelle classification. Contrairement à une modification, une mise à niveau modifie suffisamment le produit pour nécessiter un nouveau code produit. Par exemple, la mise à niveau d'une entrée sécurisée peut impliquer le remplacement de composants clés, l'intégration de technologies avancées ou l'amélioration d'éléments structurels pour répondre à des normes de sécurité plus strictes.

Efficacité énergétique et matériaux écologiques

Les entrées sécurisées modernes sont désormais équipées de moteurs écoénergétiques, de composants IoT basse consommation et de capteurs intelligents qui ajustent leur fonctionnement en fonction de l'utilisation en temps réel. Ces avancées réduisent la consommation d'énergie et améliorent l'efficacité globale des systèmes de sécurité. Les portes tournantes contribuent également à réguler le climat intérieur en limitant les échanges d'air, ce qui les rend idéales pour les projets de construction écologique et les certifications d'efficacité énergétique comme LEED. De plus, les matériaux non toxiques deviennent la norme dans la conception des entrées sécurisées.

Ces éléments contribuent à la durabilité et s'alignent sur les objectifs de responsabilité sociale des entreprises, permettant aux entreprises d'aligner leurs investissements en matière de sécurité sur les objectifs de durabilité.

Construire pour durer

Les solutions durables réduisent les déchets en minimisant les remplacements fréquents. Les entreprises délaissent les solutions miracles et adoptent des stratégies privilégiant la durabilité, la fiabilité et un impact environnemental minimal. Il ne s'agit pas seulement de relever les défis d'aujourd'hui, mais de construire pour les 100 prochaines années et au-delà. Investir dans des produits de haute qualité, conçus avec expertise, garantit des performances et une sécurité durables, ainsi qu'une expérience utilisateur fluide et durable.

5 L'EFFET VOISIN.

Gestion de la sécurité dans les immeubles à locataires multiples

Dans les immeubles multilocataires, les besoins de sécurité d'un locataire peuvent être fortement influencés par ses voisins. Que vous soyez gestionnaire d'immeuble ou locataire, il est essentiel de prendre en compte l'impact potentiel des entreprises et des occupants environnants sur vos activités. Les défis en matière de sécurité ne se limitent plus aux organisations individuelles. Par exemple, si une entreprise voisine est confrontée à des menaces – telles que des activités criminelles, des manifestations ou d'autres troubles – cela peut affecter directement votre sécurité. Ce problème, appelé « l'effet voisin », met en évidence la nature collaborative des environnements multilocataires modernes.

Équilibrer des besoins divers

Les immeubles multilocataires fonctionnent comme de petites communautés, ou des « mini-villes », où chaque locataire a des exigences et des préoccupations uniques. Certaines entreprises peuvent exiger des mesures de sécurité élevées, tandis que d'autres optent pour des options multilocataires en raison de la connectivité de leur communauté d'affaires. Cette diversité peut engendrer des tensions politiques ou des discussions animées entre les locataires, les gestionnaires d'immeubles s'efforçant de maintenir un équilibre harmonieux. Un positionnement intelligent de solutions de sécurité physique, assurant l'équilibre entre hospitalité et sécurité, peut répondre à ces défis.

L'essor de la location

Les tendances dans l'immobilier commercial montrent une transition de la propriété vers la location. Les grandes entreprises choisissent de plus en plus de louer leurs espaces plutôt que de les posséder. Cette évolution peut rendre les bâtiments plus vulnérables aux risques de sécurité liés aux locataires voisins, notamment avec l'augmentation du chiffre d'affaires et l'évolution des structures de propriété. Il est crucial pour les gestionnaires d'immeubles et les locataires d'adopter des solutions de sécurité flexibles, capables de s'adapter à l'évolution des modes d'occupation.

Menaces provenant de l'intérieur de l'organisation

Si les menaces externes dominent souvent les discussions, les menaces internes sont tout aussi importantes. Des employés mécontents ou d'anciens employés disposant de droits d'accès résiduels peuvent exploiter des vulnérabilités. Pour contrer ces risques, les entreprises ont besoin de solutions flexibles et évolutives permettant de modifier ou de révoquer rapidement les autorisations d'accès, à l'instar de la gestion des identifiants dans les environnements numériques comme les systèmes Microsoft.

La mise en place de barrières physiques, telles que des Speedlanes à certains étages, renforce la sécurité des bâtiments. Associées à l'authentification multifacteur pour l'accès numérique, ces mesures créent un système de défense complet. Leur capacité à s'adapter rapidement aux menaces émergentes, tant physiques que numériques, distingue les organisations véritablement sécurisées des organisations vulnérables.

6 IOT ET SURVEILLANCE EN TEMPS RÉEL.

L'intégration des systèmes compatibles avec l'Internet des objets (IoT) transforme la façon dont les organisations gèrent les menaces physiques et numériques. En exploitant des technologies innovantes, les entreprises peuvent assurer une surveillance continue, permettant ainsi la détection et la réponse aux risques en temps réel.

Qu'est-ce que l'IoT ?

L'IoT désigne un réseau d'appareils physiques interconnectés, équipés de capteurs, de logiciels et d'autres technologies. En collectant et en transmettant des données via Internet, ces appareils favorisent une automatisation plus intelligente et des décisions éclairées. En matière de sécurité, les applications IoT incluent la surveillance en temps réel, le contrôle d'accès et la maintenance prédictive des solutions d'entrée.

Protocole de périphérique supervisé ouvert (OSDP)

La numérisation du matériel transforme l'intégration des produits aux systèmes de contrôle d'accès, offrant ainsi plus d'efficacité et de simplicité. Traditionnellement, la connexion des appareils à ces systèmes nécessitait plusieurs câbles pour l'alimentation, la communication et le contrôle, ce qui entraînait des configurations de câblage complexes, des problèmes d'installation et de maintenance.

Cependant, des avancées comme l'OSDP simplifient ce processus en permettant des solutions monofilaires pour la communication numérique entre appareils. Au lieu de nécessiter plusieurs câbles de données, une seule connexion peut gérer plusieurs fonctions, réduisant ainsi considérablement l'infrastructure physique.

Cette interconnectivité améliorée permet aux produits de différents systèmes, tels que les systèmes de contrôle d'accès, de gestion des bâtiments et de sécurité incendie, de fonctionner ensemble de manière transparente sur une plate-forme unifiée.

En réduisant la complexité et en minimisant le risque d'erreurs lors de l'installation et de la maintenance, les opérations sont simplifiées, le temps de configuration est raccourci et la gestion globale du système est améliorée, favorisant une prise de décision et un contrôle plus fluides.

Surveillance et suivi renforcés

Les systèmes IoT offrent aux organisations des capacités de surveillance complètes 24h/24 et 7j/7. Capteurs, caméras et appareils connectés fonctionnent ensemble pour assurer un flux de données fluide et offrir une vue complète des événements de sécurité au fur et à mesure de leur évolution. Ce niveau de visibilité permet aux équipes de sécurité d'identifier et d'évaluer rapidement les menaces potentielles, leur permettant ainsi d'anticiper les failles potentielles.

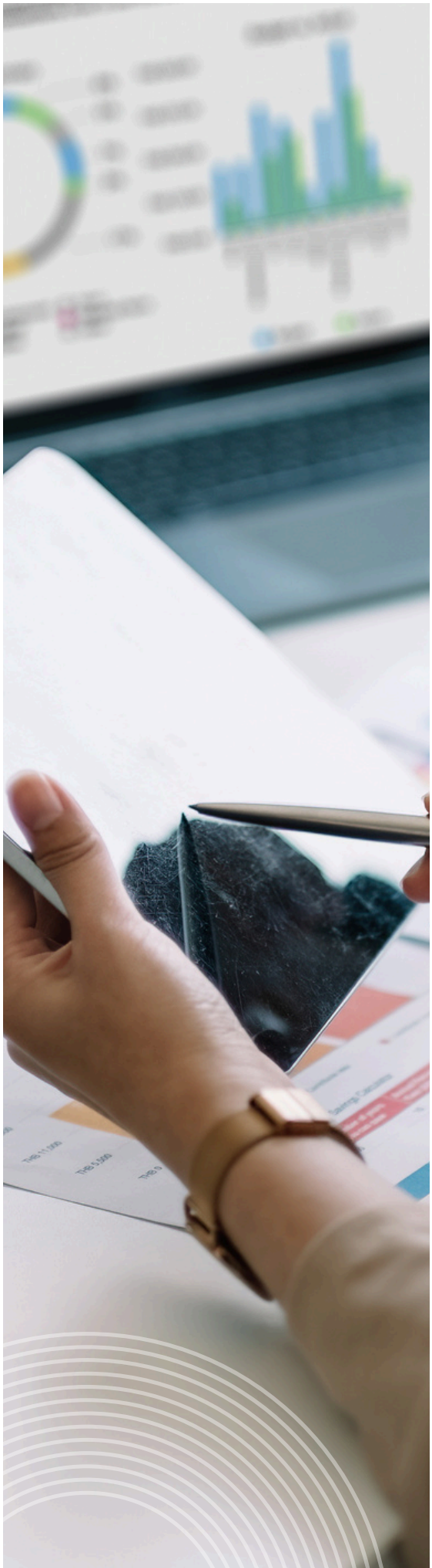
Surveillance à distance et maintenance prédictive

Dans le paysage IoT en constante évolution, la surveillance à distance et la maintenance prédictive ont révolutionné la gestion des systèmes d'accès. La surveillance à distance permet aux gestionnaires d'installations de suivre l'état et les performances des systèmes d'accès en temps réel grâce à des capteurs avancés et à une intégration logicielle sécurisée. Cette connectivité offre une visibilité immédiate sur l'état des portes tournantes, des portails de sécurité et des couloirs rapides.

La maintenance prédictive, optimisée par l'IoT et l'apprentissage automatique, optimise ce processus en analysant les tendances des données afin d'anticiper les problèmes potentiels. Au lieu d'attendre les pannes des équipements, la maintenance prédictive identifie les signes d'usure, les performances irrégulières ou les anomalies d'utilisation, permettant ainsi un entretien proactif.

Cette solution optimise les performances du système d'entrée en réduisant les temps d'arrêt, en affinant les calendriers de maintenance et en augmentant la longévité des composants clés. En traitant les problèmes avant qu'ils ne s'aggravent, les entreprises peuvent éliminer les réparations d'urgence et les interventions de service inutiles, rendant ainsi la maintenance plus rentable.

Au-delà des avantages opérationnels, la surveillance à distance et la maintenance prédictive offrent de précieuses informations basées sur les données. En collectant et en analysant les habitudes d'utilisation, les gestionnaires d'installations peuvent prendre des décisions éclairées pour optimiser l'exploitation des bâtiments et améliorer l'expérience utilisateur. Ce flux continu de données exploitables garantit la fiabilité, la sécurité et l'adaptation des systèmes d'accès aux besoins de l'installation.



L'AVENIR

AMINE BOUCHAREB

PRODUCTMANAGER - ACCÈS SÉCURITÉ

Les solutions d'entrée de Boon Edam sont conçues pour l'avenir - alliant une technologie de sécurité avancée à des conceptions flexibles et soucieuses de l'espace qui créent une expérience accueillante et sécurisée et répondent aux défis évolutifs de la sécurité moderne.

En combinant des décennies d'expertise avec une approche avant-gardiste, nous fournissons des solutions d'entrée qui protègent les actifs, améliorent l'expérience utilisateur et inspirent confiance.

L'avenir des entrées de sécurité réside dans une intégration transparente - fusionnant les défenses physiques et numériques tout en adoptant l'innovation et la durabilité.

Les organisations qui accordent la priorité à ces tendances seront bien placées pour naviguer dans un paysage de menaces de plus en plus complexe.

« L'avenir des entrées sécurisées réside dans une intégration transparente. »

UN RAYONNEMENT **INTERNATIONAL.**

Depuis près de 150 ans, nous fabriquons des solutions d'entrée sécurisées haut de gamme et élégantes aux Pays-Bas, aux États-Unis et en Chine. Forts de nos filiales établies dans les grandes villes du monde entier, nous pouvons affirmer en toute confiance que nous couvrons tous les points du globe. En outre, notre service d'exportation à l'international travaille non seulement en partenariat avec nos distributeurs mais il commercialise aussi nos produits et services en direct partout dans le monde. Ce vaste réseau nous permet d'occuper une solide position dans le monde et de bien comprendre les marchés locaux ainsi que leurs exigences uniques.

Pour trouver votre expert Boon Edam le plus proche, rendez-vous sur le site :
www.boonedam.com/fr-be/contact

Boon Edam SPRL
T +32 14 21 67 17
E be.info@boonedam.com
W www.boonedam.be/fr-be

BOON EDAM
YOUR **ENTRY** EXPERTS.