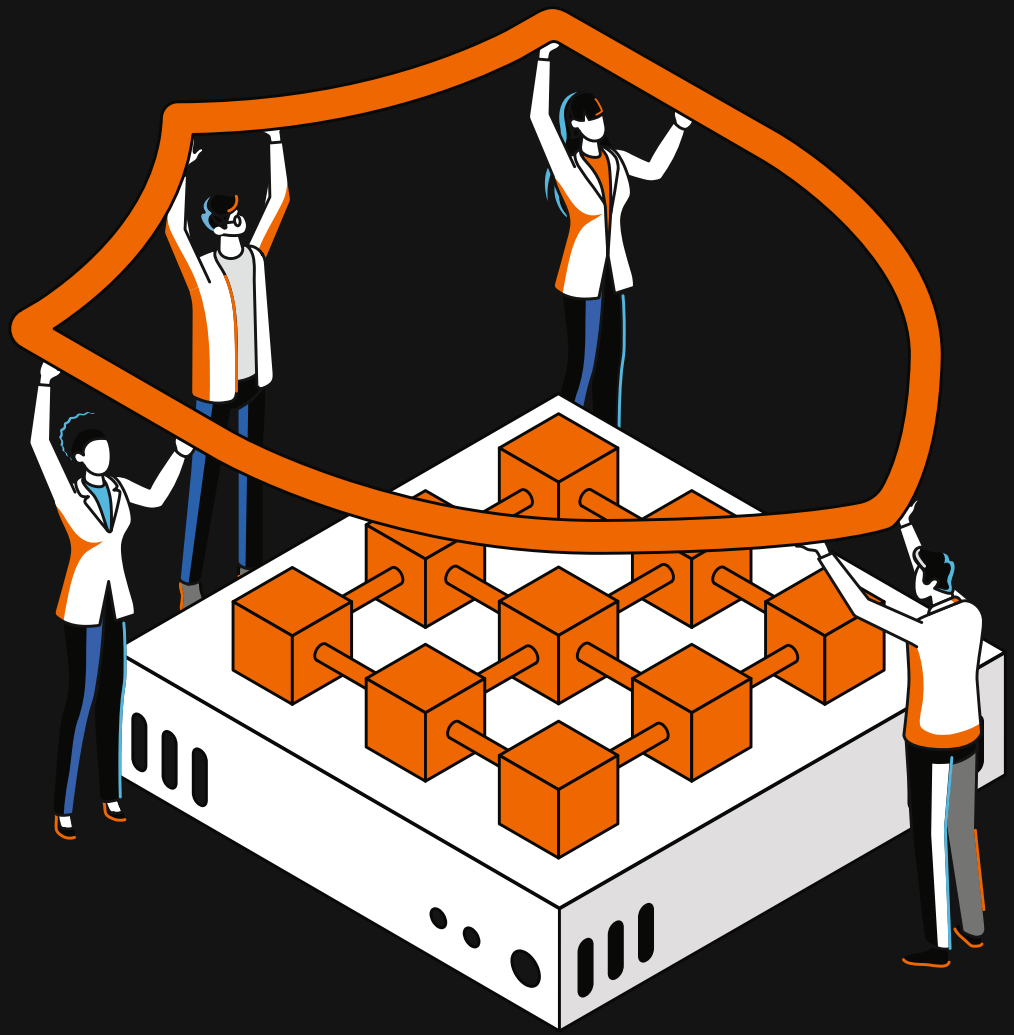
Business

Livre blanc
Sûreté-Sécurité : vers une protection globale de l'entreprise



Offrir une vision stratégique et experte sur l'évolution de la sûreté et de la sécurité dans un contexte de menaces hybrides croissantes, en intégrant les dimensions physiques, numériques et humaines.

■ Anticiper ■ Identifier ■ Protéger ■ Réagir

Un monde plus instable, plus connecté, donc plus vulnérable !

Les entreprises sont confrontées à un défi sécuritaire inédit, où crises multiples, menaces hybrides et innovations technologiques bouleversent les standards. Les responsables sûreté doivent impérativement adapter leurs stratégies pour faire face à ce risque généralisé.

Selon une étude publiée en 2025 par Proofpoint, 76 %[1] des directeurs de la sécurité des systèmes d'information (RSSI) mondiaux estiment que leur entreprise risque une cyberattaque majeure dans les 12 prochains mois, un chiffre en hausse par rapport à l'année précédente. La convergence entre DSI et sûreté est donc essentielle pour anticiper ces risques.

Menaces hybrides : un défi global pour la résilience

Les attaques ne sont plus isolées et mêlent cyber, intrusions physiques et manipulations sociales. L'intelligence artificielle, vecteur d'innovations devient aussi une arme redoutable, automatisant la fraude, la désinformation et les intrusions sophistiquées.

Les entreprises subissent ainsi une pression accrue, chaque faille pouvant impacter durablement leur réputation et leur activité.

Transformation des métiers de la sûreté

Dans ce contexte, le métier de la sûreté change radicalement. Le « gardien de site » cède la place à un « architecte de la sécurité globale », orchestrant technologies, process et ressources humaines.

Data, IoT et cloud imposent une gestion intégrée et une interopérabilité totale pour détecter et réagir en temps réel.

La coordination interservices (DSI, RH, juridique, communication) devient essentielle pour anticiper et crédibiliser la protection. Il est intéressant de noter la part des incidents qui résultent d'un mauvais usage, d'erreurs et de négligences des collaborateurs, souvent liés à des outils non approuvés ou à un manque de sensibilisation : les équipes doivent donc monter en compétences et avoir ce « jugement sûreté » afin d'éviter les vulnérabilités. La prévention, via des formations régulières et des audits, renforce l'efficacité et transforme les erreurs en opportunités d'amélioration.

Intégrer les nouvelles réglementations

Le cadre réglementaire s'intensifie : NIS2, ISO 27001, DORA, CRA. Loin d'être de simples contraintes, ces normes structurent la gestion des risques, la gouvernance des données et la gestion des incidents.

Faire appel à des partenaires maîtrisant ces exigences devient un gage d'agilité. Anticiper au lieu de subir procure aux entreprises un atout stratégique majeur dans un environnement instable.

Focus normes

NIS2
renforce la cybersécurité en Europe pour 18 secteurs stratégiques, exigeant gestion des risques, détection et notification d'incidents sous 24 h.

ISO 27001
est une norme internationale pour un management structuré de la sécurité de l'information.

DORA
cible la résilience opérationnelle du secteur financier, avec des tests réguliers.

LE CRA
impose une sécurité « by design » aux produits numériques, renforçant leur fiabilité globale.

1. Proofpoint, «2025 Voice of the CISO Report» (mars 2025)
2. https://www.cert.ssi.gouv.fr/uploads/CERTFR-2025-CTI-003.pdf

L'enjeu est clair : seules les entreprises alliant vigilance, culture de la sécurité, innovation et partenaires fiables pourront évoluer sereinement dans ce monde plus connecté et vulnérable.

L'interopérabilité des systèmes comme nouveau standard

Face aux menaces hybrides combinant cyberattaques, intrusions physiques et manipulations sociales, l'interopérabilité des systèmes devient un standard incontournable pour la sûreté des entreprises. En intégrant vidéosurveillance, contrôle d'accès (ex. : badges mobiles) et connectivité adaptée, les plateformes interopérables permettent une gestion unifiée des risques.

En 2024, plus de la moitié[2] des opérations de cyberdéfense de l'ANSSI ont eu pour origine des vulnérabilités sur les équipements de sécurité en bordure de SI (comme les systèmes d'accès physiques dans les bâtiments), amplifiant les risques hybrides dus à des silos non intégrés. Ce constat alarmant appelle à une action immédiate pour une résilience unifiée, conforme NIS2.

Le + d'Orange Business

Avec 6000 experts en cloud et cybersécurité, nous accélérons la transformation numérique des entreprises via des solutions innovantes et souveraines. Appliquant les recommandations ANSSI, nous supervisons 24/7 vos environnements hybrides pour une sécurité renforcée.

Hypervision :
Comment choisir votre système de contrôle ?

Les infrastructures de sûreté fédérées par un hyperviseur constituent une cible de choix pour les attaquants. Leur compromission ouvre potentiellement l'accès à l'ensemble des données et traitements hébergés, ce qui oblige à considérer à la fois les menaces d'origine physique que celles issues de la cybercriminalité lors de la mise en place d'une infrastructure supervisée.

En fonction du type de menace, les motivations peuvent varier : volonté d'espionnage, de vol de données ou d'intrusion physique, avec des motivations financières, géopolitiques ou idéologiques.

Une configuration inadéquate de ces systèmes de supervision accroît considérablement le risque d'intrusion dans les infrastructures critiques, il est donc crucial de s'appuyer sur un intégrateur expérimenté afin de garantir la sûreté de l'environnement bâti.

Une analyse préalable et rigoureuse permet d'identifier précisément les besoins, d'optimiser les coûts et d'assurer une maintenance pérenne.

VMS ou hyperviseur ?

Un **VMS** (Video Management System) est généralement déployé lorsqu'il s'agit de centraliser et d'exploiter exclusivement les flux issus des caméras de vidéoprotection.

Il assure la collecte, le stockage, la supervision et, dans certains cas, l'analyse des images. En revanche, dès lors qu'une organisation souhaite aller au-delà de la gestion vidéo et intégrer d'autres briques de sécurité (contrôle d'accès, détection d'intrusion, interphonie, systèmes IoT), le recours à un **hyperviseur** s'impose. Celui-ci agit comme une plateforme logicielle fédératrice, permettant de corréler les événements entre systèmes hétérogènes et de disposer d'une vision unifiée de la sûreté du site.

+15 %

En France, les cyberattaques ont augmenté de 15 % en 2024 d'après l'ANSSI, la réussite de ces attaques sont de plus en plus souvent liées à des vulnérabilités physiques mal prises en compte dans les analyses de risques cyber ; un hyperviseur unifié pourra fortement contribuer à réduire ces risques, renforçant la résilience face aux menaces hybrides.

Encore faut-il que cet hyperviseur soit déployé selon les règles de l'art : choix d'un intégrateur qualifié, configuration sécurisée, et prise en compte des recommandations de l'ANSSI afin de limiter les risques de compromission et d'assurer la pérennité de l'infrastructure.

Chez Orange Business, nous jouissons d'une réelle expérience et maîtrise en la matière. En effet, nous sommes en cours de déploiement et d'intégration d'un hyperviseur de Sécurité afin de superviser tout type d'alarme, pour l'ensemble des sites français d'un groupe du CAC40. Afin, à terme, de permettre à notre centre opérationnel de pouvoir gérer toutes les alarmes en 24/7.

CHRISTOPHE CHAUSSECOURTE, SENIOR BUSINESS DÉVELOPPER.

■ identifier ■ dimensionner ■ localiser ■ interconnecter ■ exploiter

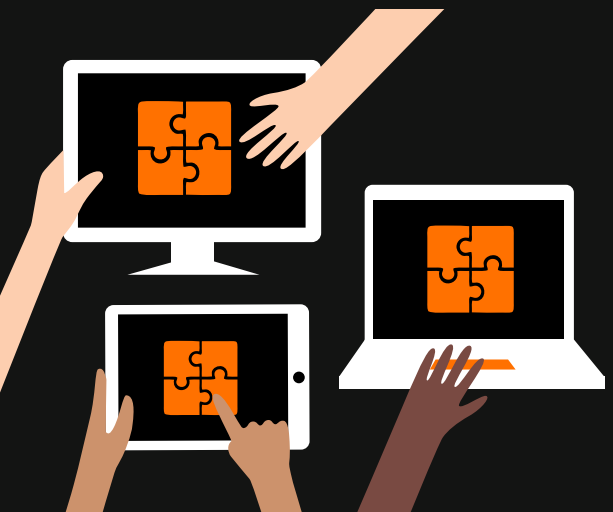
Hypervision :
Comment choisir votre système de contrôle ?

Simplifier le quotidien de vos équipes

Une Hypervision unifiée simplifie le quotidien des opérateurs, techniciens et responsables sûreté. Une console centralisée et des tableaux de bord clairs remplacent la dispersion d'outils, limitant les erreurs humaines dues à des configurations complexes. Les alertes sont corrélées et dédoublonnées, augmentant l'efficacité opérationnelle, tandis que des scénarios types (porte forcée, incendie) guident les gestes en temps réel.

La synchronisation avec les RH et Services généraux (badges mobiles, visiteurs), complétée par une maintenance continue et proactive, sécurise les accès sans interruption.

Les équipes gagnent ainsi du temps, passant de la gestion de crises à la prévention et à la formation continue..



Maintenance et pérennité des hyperviseurs

La pérennité d'un Hyperviseur repose sur une maintenance rigoureuse et une évolutivité sans régression, essentielle pour protéger vos bâtiments des menaces en constante mutation.

Un Maintien en Condition Opérationnelle (MCO) sur plusieurs années garantit la résilience en évitant l'obsolescence, un risque majeur pour les infrastructures sensibles. Des mises à jour régulières et une supervision proactive assurent une disponibilité continue, même face à des imprévus. Une approche structurée avec tests préalables offre une base solide pour une sécurité durable.

De plus, **une maintenance proactive** prévient l'apparition de nouvelles vulnérabilités exploitable par un attaquant, limitant ainsi la surface d'attaque et réduisant les risques d'intrusions.

3 fois plus cher

Selon ProTech Security, une panne inattendue coûte 2 à 3 fois plus cher qu'une intervention planifiée, incluant frais urgents et main-d'œuvre. Une détection précoce réduit à la fois les coûts opérationnels et garantit un système fiable et répondant aux objectifs de sécurités recherchés.

La check-list pour élaborer votre architecture de contrôle d'accès ou vidéoprotection

Analyse de sûreté du site :

- Identification des zones de valeur
- Mise en place d'une stratégie de protection par définition de zones concentriques – augmentation de la sûreté plus on se rapproche des zones de valeur
- Définition des solutions techniques à mettre en œuvre

Définition des règles métiers de la sûreté :

- Identification des processus de supervision, ergonomie du poste de travail et formation
- Définition des scénarios de corrélation des alarmes et d'identification des signaux faibles
- Définition des processus d'intervention, de consignation et de mise en sécurité
- Consigner, analyser et informer

Prise en compte des contraintes d'intégration :

- Identification des locaux de mise en œuvre ainsi que les contraintes d'installation sur le bâtiment
- Identification du réseau de sûreté, des accès à la solution ainsi que des interconnexions
- Définition de la politique de cybersécurité à mettre en œuvre

■ identifier ■ dimensionner ■ localiser ■ interconnecter ■ exploiter

Un contrôle d'accès 2.0 ?
Pack ID Mobile ou wallet ?

Quid de la sécurité des données ?

Le contrôle d'accès n'est pas exempt, lui aussi, des tendances technologiques qu'il faut connaître et maîtriser pour être certain qu'une fois l'arbitrage technique fait, la solution retenue corresponde aux besoins et contraintes de l'utilisateur final.

CLAUDE FOULLON, RESPONSABLE DES SOLUTIONS SÉCURITÉ ET SÛRETÉ, ORANGE BUSINESS.

Les solutions de contrôle d'accès mobile, comme les wallets (Apple, Google), permettent une gestion pratique des identifiants via smartphone, facilitant l'accès pour les employés ou visiteurs. Cependant, partager sans contrôle réel par l'entreprise des données sensibles, telles que des identifiants de services, les historiques d'accès, ou de localisation, avec des plateformes tierces expose à des risques de fuites ou de non-conformité avec le RGPD.

Bien souvent, les violations de données impliquent des identifiants mal protégés, souvent liés à des clouds non sécurisés. Les recommandations de l'ANSSI exigent un contrôle strict de la localisation et du traitement des données, ce qui peut être compromis par des infrastructures hébergées hors UE, soumises à des lois comme le Cloud Act américain.

L'adoption d'un cloud souverain, hébergé dans l'UE, garantit la maîtrise des données et la conformité réglementaire, réduisant ainsi les risques.

Conçu pour le contrôle d'accès physique

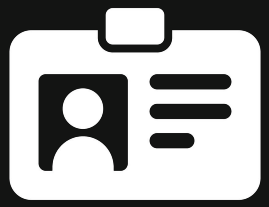
Conçu pour les environnements professionnels, ces solutions dédiées au contrôle d'accès physique, dématérialisent les badges sur smartphone, s'intègrent aux lecteurs existants (13,56 MHz), et offrent une gestion en temps réel des autorisations avec un chiffrement avancé.

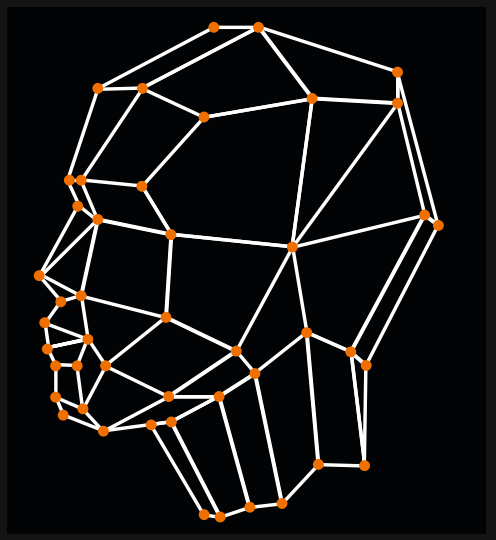
On pourra lui conseiller, une approche type Pack ID Mobile d'Orange Business, une solution très sécurisée conçue spécifiquement pour le contrôle d'accès physique. Elle permet de dématérialiser les badges et les données biométriques sur smartphone, fonctionne avec la plupart des lecteurs du marché et offre une gestion en temps réel des identifiants de services. De plus, elle assure une intégration simplifiée avec les infrastructures des clients, tout en renforçant la sécurité et en facilitant la gestion des utilisateurs.

CLAUDE FOULLON, ORANGE BUSINESS.

Gestion simple et sécurisée

Le Pack ID Mobile d'Orange Business conviendra particulièrement aux organisations cherchant à conserver la maîtrise de l'ensemble de leurs données de sécurité sans nécessiter de développements importants. Les wallets des constructeurs (Apple, Google, Samsung…) seront plus pertinents pour des usages « grand public » ou pour des contrôles d'accès physique à faible contrainte réglementaire.





Sur le terrain

Digitaliser le contrôle d'accès permet d'automatiser certaines tâches.

Orange Business est capable de déployer un dispositif de vérification de la pièce d'identité et d'authentification du porteur par biométrie 3D faciale. En effet, les fonctions d'accueil des visiteurs et des intervenants sont parmi celles que les nouvelles technologies permettent de digitaliser. Les ressources humaines qui y sont consacrées peuvent être ainsi allouées à d'autres missions. Grâce au système, conçu **en partenariat avec One Visage**, nous pouvons authentifier automatiquement le porteur d'un titre d'identité lorsqu'il se présente à l'entrée du site, et lui fournir un badge d'accès en temps réel. Un tel outil pourrait être mis à disposition de l'accueil des personnes travaillant sur le site la nuit où lorsqu'il est fermé afin de le délivrer automatiquement un droit d'accès correspondant à leurs habilitations, leurs formations ou qualifications… pour intervenir dans telle ou telle zone, accéder à telle ou telle partie du site.

Il s'agit d'un système très efficace, rapide et performant, qui permet de gérer de manière fluide et sécuriser les visiteurs récurrents d'un site.

La connectivité :
les clés pour sécuriser vos bâtiments

La connectivité transforme la sûreté des bâtiments, portée par l'essor de l'IoT, des réseaux 5G et les data centers. Cependant, elle introduit des risques nouveaux, comme les failles potentielles dans les systèmes connectés ou la dépendance à des infrastructures externes. Dans un contexte de menaces élevées et d'exigences renforcées, sécuriser les réseaux devient un pilier de la sûreté des bâtiments. Comment protéger vos actifs en choisissant les bons réseaux et en garantissant la résilience de vos systèmes ?

Sécuriser objets connectés et données

Les objets connectés, tels que les caméras ou les capteurs, enrichissent la surveillance, mais peuvent être des points d'entrée pour des intrusions.

Des mesures de sécurité, comme le chiffrement des communications, et l'authentification renforcée (802.x) sont fortement recommandées par L'ANSSI afin de protéger les données partagées par ces dispositifs. La confidentialité des données en transit doit être garantie par des protocoles sécurisés. Par exemple, isolez les flux vidéo des systèmes critiques pour éviter une compromission en chaîne.

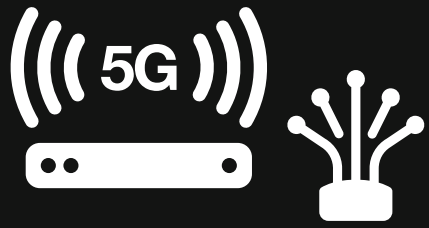
Une faille dans un seul appareil pourrait affecter l'ensemble de votre système de sûreté.

Les data centers : cœurs de la circulation et de la protection des données

La connectivité réseau joue un rôle central pour transporter les données issues des objets connectés vers des data centers, où elles sont stockées,traitées et distribuées de manière sécurisée. Ces datas centers agissent comme des hubs essentiels, garantissant que les informations collectées par vos caméras, capteurs ou systèmes de surveillance arrivent rapidement et en toute fiabilité pour une analyse en temps réel. Plus le chemin de transport de la donnée est court, par exemple avec un serveur local hébergé dans le même bâtiment et connecté via un réseau LAN, plus la latence est réduite et la connexion est fiable, minimisant les risques de perturbations.

73 %

Selon IDC, 73 % des entreprises investiront davantage dans l'analyse de données, soulignant l'importance de processus continus et sécurisés.



Choix des réseaux

5G publique, privée, hybride ou fibre optique ?

Le choix du réseau impacte directement la sécurité et la performance.

5G publique

offre une solution rapide à mettre en place, mais ses ressources étant partagées entre l'ensemble des utilisateurs, ce réseau peut présenter des risques de congestion susceptibles d'affecter la disponibilité et la qualité de service.

5G privée

garantit un environnement isolé, parfait pour les sites sensibles nécessitant une haute sécurité.

5G hybride

combine les avantages des deux avec une couverture élargie, en isolant les données critiques tout en utilisant le réseau public pour des usages moins prioritaires.

Fibre optique

en tant que solution filaire, assure une connexion ultra-fiable et sécurisée pour les bâtiments fixes, avec une faible latence et une résistance aux interférences, idéal pour supporter les flux de données importants.

La connectivité :
les clés pour sécuriser vos bâtiments

Pour assurer la résilience, optez pour des technologies redondantes comme la fibre optique, qui réduisent les latences et les pannes, tout en offrant une haute disponibilité. Dans un monde toujours connecté, les réseaux doivent transporter de grands volumes de données de façon fiable, permettant une analyse 24 h/7 j indispensable à la sûreté. Protégez ces flux en isolant les données critiques, en utilisant des protocoles de chiffrement robustes et en intégrant des backbones réseaux privés pour éviter les intrusions externes.

Ainsi, vous renforcez la maîtrise de vos actifs, en combinant performance et protection contre les menaces croissantes.

Implications des choix technologiques

Les choix de connectivité influencent le budget, la performance et la résilience.

Un **réseau privé**, ou une **infrastructure filaire** nécessitent un investissement initial plus élevé, mais il peut réduire les coûts d'exploitation en contrôlant la qualité de service, la confidentialité des flux sensibles et la maintenance.

Le recours à des **réseaux publics**, comme la **5G** ou le **Wi-Fi professionnel**, s'avère souvent plus rapide et économique, à condition de bien encadrer les engagements de service : disponibilité, couverture, priorisation du trafic, délais d'intervention et de rétablissement.

Un **modèle hybride**, combinant fibre pour les flux critiques, 5G publique pour la mobilité et réseaux bas débit longue portée pour les capteurs, représente un bon compromis si les flux sont clairement cloisonnés et supervisés.

Quel que soit l'arbitrage, il faut prévoir la redondance des liaisons, le fonctionnement en mode dégradé, l'authentification forte des équipements, le chiffrement des communications et la conformité au cadre européen, par exemple NIS2 ou le règlement sur la résilience cyber. Enfin, décider sur la base d'essais sur site et d'un coût total de possession incluant énergie, maintenance et support permet d'éviter les effets de bord à long terme.

99,9985 %

C'est le taux de disponibilité du réseau fibre d'Orange.

30 ans

d'expérience dans la sécurisation d'infrastructures vitales.

24/7

Nos centres opérationnels surveillent l'état du réseau en continu pour garantir votre haute disponibilité.

Leader 2025

Orange Business est reconnu leader par Gartner dans son premier Magic Quadrant™ for 4G and 5G Private Mobile Network Services.

Donneurs d'ordres publics et sites sensibles
Les réponses d'Orange Business à vos problématiques

OIV/OSE

Les opérateurs d'importance vitale (OIV) et opérateurs de services essentiels (OSE) font face à des menaces croissantes, notamment cyber.

Orange Business les accompagne avec des solutions robustes : renforcement de la résilience des systèmes d'information (SI), cybersécurité avancée, intégration de l'IA pour la détection proactive, optimisation de la performance opérationnelle, modernisation des environnements de travail et expertise en transformation numérique. Ces services garantissent une sécurité continue et une adaptation aux défis actuels.

Les bailleurs sociaux et collectivités locales

Qu'il s'agisse des bailleurs sociaux ou des collectivités locales, ces donneurs d'ordres font face à de nombreuses problématiques sécuritaires.

Allant des incivilités (dégradations, squats de zones publics, dépôts sauvages de déchets…) aux agressions, en passant, évidemment par les trafics liés à la drogue ou autres. Les caméras mobiles constituent aujourd'hui une réponse technique pertinente pour lutter contre ces phénomènes. Adaptées à la surveillance temporaire ou évolutive, facilitant le déploiement rapide lors d'événements ou en zones sensibles, leurs données remontées en temps réel, centralisées de manière sécurisée permettent de réagir rapidement. Par ailleurs, elles jouissent d'un ROI bien plus efficace que les caméras fixes. Grâce à l'IoT, à l'analyse vidéo intelligente et à une gestion flexible des accès, Orange Business vous aide à prévenir les incivilités, protéger les habitants, tout en garantissant la confidentialité et la conformité réglementaire.

Les collèges/lycées

Le monde scolaire n'est malheureusement pas à l'abri des incivilités, des violences, des intrusions…

Là encore, la maîtrise des solutions flexibles de contrôle d'accès et des technologies de la vidéoprotection par les équipes d'Orange Business sera un atout dans vos projets. En outre, Orange Business pourra vous accompagner pour mettre au service de la sécurité de ces sites l'IA qui permet de détecter automatiquement les intrusions, comportements suspects ou situations à risque dans les établissements scolaires inoccupés, grâce à l'analyse en temps réel des images des caméras… afin d'optimiser la prise de décision et la rapidité d'intervention en cas d'incident.

Établissements de Santé

Cabinets médicaux, cliniques, hôpitaux publics… sont aussi menacés.

Orange Business sécurise l'accès aux hôpitaux via des solutions d'identification, de badges personnalisés, la gestion centralisée des autorisations et la traçabilité des accès. Ces services permettent de protéger patients, personnels et données sensibles, tout en respectant les normes strictes de confidentialité hospitalière.

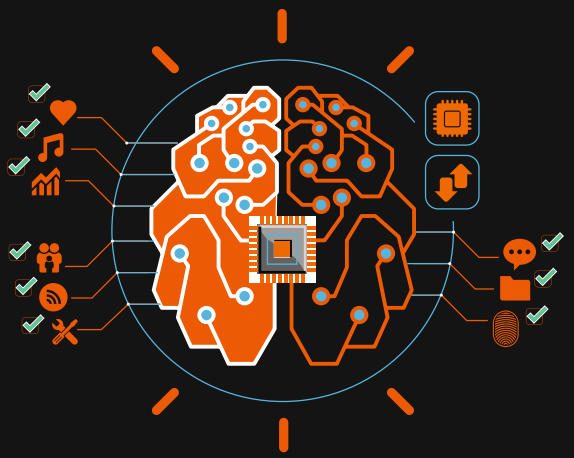
Dépasser la simple logique d'installation
La sûreté qui s'exploite

L'avenir de l'IMSE (installateur mainteneur de sûreté électronique) repose sur des plateformes dynamiques offrant un suivi en temps réel et une transmission complète du savoir. L'IA y trouve sa place pour capitaliser l'expérience des projets et éviter la perte de connaissance liée au turnover.

L'intégrateur comble un vide critique

Être intégrateur-mainteneur de sûreté électronique aujourd'hui, c'est proposer un service "sans couture", du design à la maintenance, au service d'un client acteur et non simple utilisateur. Un bon intégrateur dépasse désormais la logique d'installation : il devient partenaire, capable de mobiliser des profils transverses et des expertises variées – réseau, cloud hybride, convergence OT/IT, cybersécurité et résilience.
Alors que beaucoup de DSI ont migré vers le cloud et perdu des compétences sur les SI bâtimentaires et industriels, l'intégrateur comble ce vide critique.

ALEXANDRE FOUSSE, PRÉSIDENT ET ASSOCIÉ FONDATEUR DE STRAAD.A.



Faire du multisite

L'intégrateur, pour certains marchés, sera aussi utile grâce à sa capacité à gérer les problématiques multisites.

Dans le cas des lycées, des collectivités, par exemple, s'appuyer sur un intégrateur qui maîtrise tous les enjeux techniques de la sûreté permettra de "flécher" toutes les solutions déployées vers un centre opérationnel mutualisé. Ses retours d'expérience garantiront le choix des bonnes technologies et leur usage dans les meilleures conditions opérationnelles et de cybersécurité.

VIRGILE AUGÉ, DIRIGEANT D'ACO CONSEIL.

Garantir pérennité et sécurité

Côté donneur d'ordre, il s'agit de reconnaître cette valeur en budgétisant une véritable activité de pilotage transverse, portée par des experts capables de dialoguer avec la DSI, la compliance et les équipes cyber. En concertation avec l'IMSE, la prise en main des sites devient un transfert progressif, garantissant pérennité et sécurité.

ALEXANDRE FOUSSE, PRÉSIDENT ET ASSOCIÉ FONDATEUR DE STRAAD.A.

Choisir ses combats, avancer par étapes

Vous ne pourrez pas tout traiter, et ce n'est ni réaliste ni nécessaire. L'enjeu est de passer d'une liste infinie de vulnérabilités à deux dynamiques complémentaires et pilotables :

atténuer les menaces sur les systèmes réellement exposés et réduire le risque global de l'organisation.

- **Commencez par un état des lieux lucide et partagé.**
- **Cartographiez vos actifs et dépendances critiques.**
- **Qualifiez votre surface d'attaque externe.**
- **Vérifiez le maintien en condition opérationnelle de vos briques clés.**
- **Alignez risques, impacts et responsabilités entre sûreté, DSI et métiers.**

Un intégrateur de confiance comme Orange Business vous accompagne de bout en bout : état des lieux et priorisation, architecture et intégration, sécurisation et exploitation, conformité et souveraineté.
L'essentiel n'est pas d'être partout, mais d'avancer, de mesurer et d'ajuster : étape après étape, vous gagnez en sécurité et gardez la maîtrise.

Vers une sécurité intégrée et résiliente
Pourquoi choisir Orange Business ?

Intégrateur réseaux et numérique de confiance

Un facilitateur

Agir comme un facilitateur et un intégrateur de solutions complexes, en mobilisant l'ensemble des compétences du groupe.

Besoins spécifiques des clients

Adapter et personnaliser les offres en fonction des besoins spécifiques des clients.

Gestion des projets

Assurer la gestion de projets, notamment en matière de sécurité, de communication et d'infrastructure.

Conformité et performance

Collaborer étroitement avec les partenaires et la direction sécurité du groupe pour garantir la conformité et la performance des solutions proposées.

Apporteur de solutions

Se positionner comme un acteur de référence, capable d'apporter des solutions innovantes et adaptées aux enjeux.