

KONICA MINOLTA

E-BOOK :
COMMENT CHOISIR
SA SOLUTION DE
VIDÉOPROTECTION ?



Giving Shape to Ideas
La passion de l'innovation

Introduction

Le rôle d'un système de vidéoprotection

La sécurité est une des priorités de toutes les entreprises qui souhaitent protéger leurs personnels, leurs biens et leurs sites. Elles ont alors besoin de systèmes intelligents capables d'assurer leur sûreté, et de garantir à leurs employés un cadre de travail serein. Les départements sécurité des entreprises qui souhaitent remplir cette

mission s'équipent d'un système de vidéoprotection. Mais le marché regorge de solutions, alors comment sélectionner le bon système ? Il s'agit en premier lieu de définir précisément son rôle, en fonction du site concerné et du besoin de l'utilisateur, d'appréhender les écueils des solutions «low cost», de sélectionner les fonctionnalités

en fonction des besoins, notamment grâce aux technologies de pointe telles que l'intelligence intégrée, et de s'assurer que la solution choisie fournit une protection contre tous les risques numériques.

Vidéosurveillance

Les dispositifs dits de « vidéosurveillance » concernent des lieux non ouverts au public (locaux professionnels comme les bureaux ou les réserves des magasins) et sont soumis aux dispositions de la loi « Informatique et Libertés ». [Glossaire de la CNIL](#)

Vidéoprotection

Les dispositifs dits de "vidéoprotection" filment la voie publique et les lieux ouverts au public et sont soumis aux dispositions du code de la sécurité intérieure. [Glossaire de la CNIL](#)



1/ Le rôle d'un système de vidéoprotection

Les rôles d'un système de vidéoprotection peuvent être multiples :

- **Dissuader les auteurs potentiels de dégradations** : la présence d'une caméra, ou la diffusion d'un message vocal lors de la détection d'une présence peut décourager les auteurs de certaines dégradations.
- **Assister les opérateurs de sécurité à la gestion des flux entrants et sortants** (personnel, véhicules) afin d'identifier les comportements inhabituels.
- **Détecter des objets ou des individus** afin d'identifier des événements malveillants.
- **Détecter des catastrophes naturelles** comme les inondations ou les incendies
- **Aider à la surveillance des valeurs d'une entreprise** : lorsqu'un agent de surveillance, situé à un poste de sécurité, ne peut avoir dans son champ de vision toute la zone placée sous sa responsabilité.
- **Lever le doute en cas d'alarme ou d'intrusion sur un site** : afin d'éviter les interventions humaines inutiles si l'alarme n'est pas liée à un problème de sécurité (c'est-à-dire une fausse alarme).
- **Participer à l'investigation après une infraction** : les enregistrements des images permettent de constituer des faisceaux de présomption pour prouver un vol ou une dégradation ou pour retrouver ou confondre leurs auteurs.



2/ Quels sont les critères fondamentaux pour bien choisir une solution de vidéoprotection ?

La solution doit être choisie en fonction du rôle conféré au système de vidéoprotection de l'entreprise. On choisira alors un ou plusieurs types de caméra parmi celles-ci :

- **Caméra d'intérieur** : elle doit fournir une vision adaptée à l'objet (individu, véhicule, flux, etc.) de la vidéosurveillance : hémisphérique à 360°, panoramique à 180°, ou des angles de saisie allant de 103° à 15° pour l'identification.
- **Caméra d'extérieur** : Les caméras doivent fonctionner idéalement dans tous les environnements climatiques et maintenir leur qualité de restitution des couleurs et contrastes lorsqu'elles sont exposées aux influences environnementales. L'enveloppe

de la caméra doit protéger celle-ci de façon optimale et offrir une très haute qualité d'image de jour et de nuit selon la vision souhaitée.

- **Caméra thermique** : dans l'obscurité totale, elle doit détecter des personnes ou objets en mouvement de manière très précise, et les sources de chaleur potentiellement mortelles (en cas d'incendie).
- **Caméra dôme mobile** : motorisée et dirigée par un opérateur, elle doit identifier des détails décisifs, à distance, et doit pouvoir être pivotée ou inclinée pour couvrir les zones à surveiller et protéger tout en fournissant une haute résolution d'image.

- **Caméra portique** : positionnée sur les entrées, les portes et portails, elle doit permettre de, via un terminal vidéo et un système modulaire, déverrouiller les portes en toute sécurité et protéger les accès.

- **Les caméras nomades** : Il s'agit d'un dispositif de caméra de surveillance complet, généralement sous forme de borne intégrant la caméra, le moyen télécom et une batterie. Il peut être installé sur un mur, un éclairage public ou un véhicule.

En fonction des besoins, les caméras peuvent être discrètes (seul l'objectif peut être visible), semi-discrètes (montées en saillie et encastrées), ou dissuasives (clairement visibles).



Pour être fiables et sécurisées, les caméras doivent pouvoir :

- **Résister à des conditions climatiques et températures extrêmes**, se passer de chauffage ou de ventilation, ne pas être soumises aux effets de la condensation, de la corrosion, de la pollution et de l'exposition directe au soleil.
- **Identifier des individus** : une cible humaine doit avoir une taille d'au moins 100% de la hauteur de l'écran.
- **Fournir une performance minimale en faible éclairage**, en contre-jour, et en capture d'image de cible mobile.

- **Protéger les enveloppes de caméra** afin de conserver la même qualité d'image en cas de projection d'eau ou d'immersion temporaire ou prolongée de la caméra.

- **Être marquées par les informations relatives au fabricant** et documentées avec toutes les instructions concernant l'installation des systèmes vidéo.

Elles doivent aussi être bien placées : plus l'angle de vue est large, moins les capacités de zoom numérique sont performantes. Il faut alors choisir la bonne optique, veiller à bien positionner la caméra sur l'emplacement et l'angle de vue pour chaque caméra de surveillance ou de protection :

- À un endroit où aucun obstacle ne viendra s'interposer entre l'objectif et la cible
- Aux points de passage obligés (entrées, sorties)
- Dans des zones sensibles (archives de documents confidentiels, coffre-fort, etc.)
- Dans tout autre lieu en fonction des besoins de l'entreprise

Par ailleurs, afin d'assurer une protection optimale, les caméras de type panoramique ou hémisphérique permettent de couvrir plusieurs directions.



3/ Quelle est la valeur ajoutée de l'intelligence intégrée ?

Une caméra qui gère les enregistrements, le traitement d'images, et les alarmes forme un système complet et autonome. Il embarque une intelligence au service de la vidéoprotection.

Cette intelligence permet de :

- **Analyser en temps réel** les mouvements des personnes et des objets pour éviter les fausses alertes
- **Anticiper les comportements** grâce à la génération de rapports automatiques des activités régulières
- **Détecter les comportements douteux**, notamment dans l'obscurité totale, et automatiquement déclencher des actions (message sonore, appel téléphonique, alarme visuelle, enregistrement vidéo, transfert de données, ouverture de barrières, etc.)
- **Traiter les détections plus rapidement** et surtout alléger la charge des flux vidéos sur l'infrastructure réseau.



4/ Que cachent les solutions « low-cost » ?

Les solutions « low cost » (ou à bas prix) ne peuvent garantir un système de surveillance et de protection suffisamment robuste, fiable, et sécurisé. Pour implémenter un système performant, il convient en effet de viser un certain niveau d'exigence.

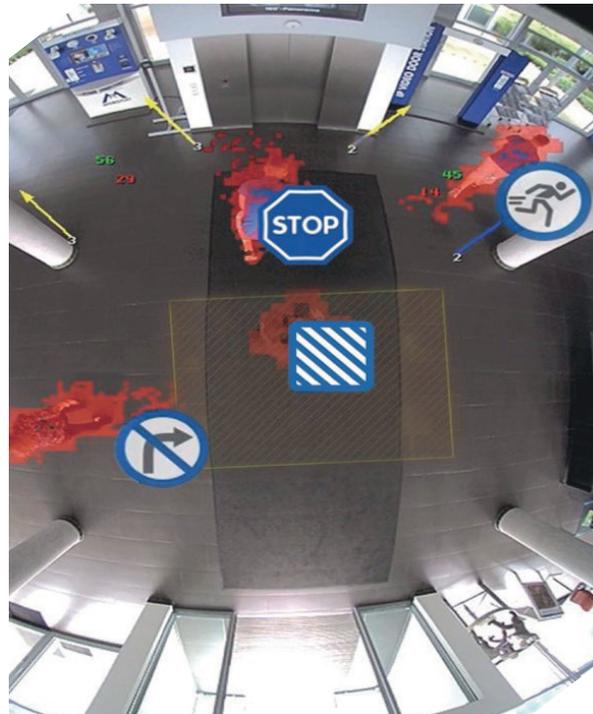
Qu'exiger en matière de qualité d'image ?

La capture d'image est un élément clé en matière de vidéoprotection. Elle est déterminée par la qualité des composants du système optique de la caméra, de la résolution de l'image et du traitement logiciel embarqué dans la caméra intelligente.

Les éléments à prendre en compte sont :

- **La qualité de l'optique et du capteur de la caméra**
- **Le niveau de sensibilité de la caméra**, c'est à dire la quantité de lumière nécessaire pour un bon fonctionnement du capteur

- **La capacité de la focale** (pour déterminer la taille de l'image de la cible) et la cible pour atteindre l'objectif de prise de vue « Identifier », tel que défini et utilisé dans la CNPP R82, dans les normes relatives à l'installation de système de vidéosurveillance et dans l'arrêté du 03 Août 2007.



Qu'exiger en matière de plateforme d'enregistrement ?

Pour identifier tout ou partie du mode opératoire d'un acte malveillant, l'enregistreur doit pouvoir restituer toutes ses séquences avec précision.

Il doit alors permettre de :

- Stocker une grande quantité de données
- Extraire des photos de haute résolution
- Préserver le niveau de définition
- Traiter les images
- Rechercher des séquences, ou les effacer
- Permettre les recherches à posteriori
- Fournir une interface intuitive pour l'utilisateur

Qu'exiger en matière de qualité et de fiabilité des équipements ?

Avant tout achat d'équipement il faut s'assurer que l'origine de fabrication des équipements est traçable, qu'il soit capable de gérer des conditions météorologiques extrêmes pour les positionnements extérieurs, et que son MTBF (Mean Time Before Failure – moyenne de temps avant panne) soit suffisant. Il s'agit aussi de s'assurer que le système n'est pas limité en termes de nombre d'utilisateurs et de caméras.

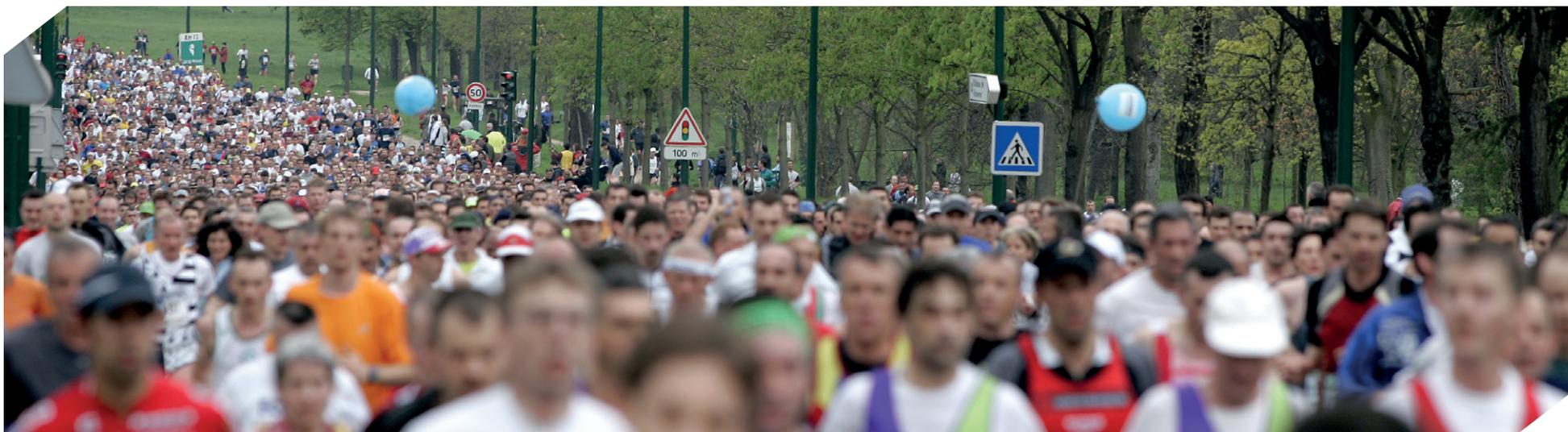
Qu'exiger en matière de sécurité du système ?

La sécurité du système comprend :

- **L'intégrité du système** : il doit posséder des fonctionnalités de détection de faille, de protection contre les accès frauduleux et non autorisés.
- **L'intégrité des données** : il doit posséder des fonctionnalités d'identification, d'authentification, et de protection des données.

Cette protection de bout en bout permet de se protéger des cyberattaques et des vols de données.

MTBF. Il existe une différence notable entre un produit peu cher mais qui a une durée de vie de 20 000 heures et un autre plus onéreux mais qui fonctionne durant 80 000 heures. Pour des caméras qui fonctionnent 24 heures sur 24, le système « low cost » a en fait un coût plus élevé sur le long terme.

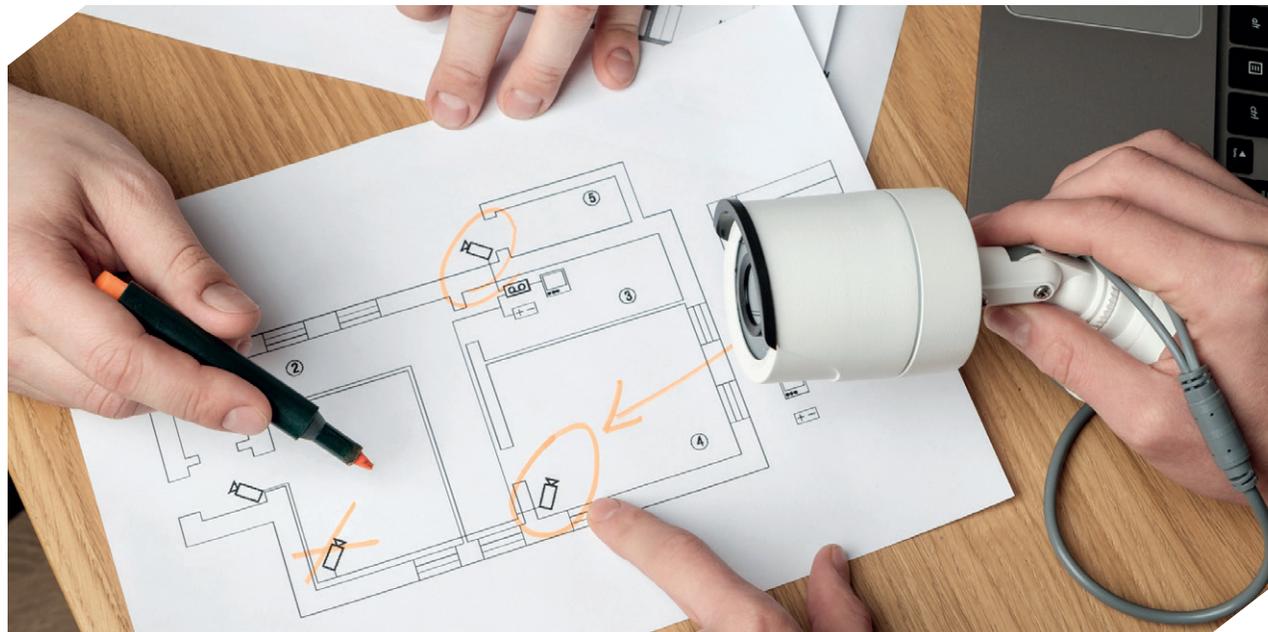


5/ Quelle architecture choisir pour pérenniser son investissement ?

Pour garantir une simplicité d'utilisation tout en étant performante, une plateforme de vidéoprotection doit avoir une architecture adaptée. L'approche centralisée – c'est-à-dire avec un ordinateur central, un serveur externe, et des licences logicielles de surveillance – ne peut supporter la charge de traitement nécessaire au stockage et

traitement d'images numériques, et bloquerai tout le système en cas de panne. Implémenter un dispositif décentralisé est alors la meilleure solution. Car l'enregistrement s'effectue directement dans la caméra IP vers l'enregistreur. Elle intègre une fonction logicielle interne à la caméra d'enregistrement qui sauvegarde les données

sur une carte SD interne ou sur un disque dur externe, et est dotée d'un logiciel de vidéosurveillance qui gère directement les alarmes et les données.



Une caméra IP est une caméra de surveillance utilisant le Protocole Internet pour transmettre des images et des signaux de commande via une liaison Fast Ethernet.

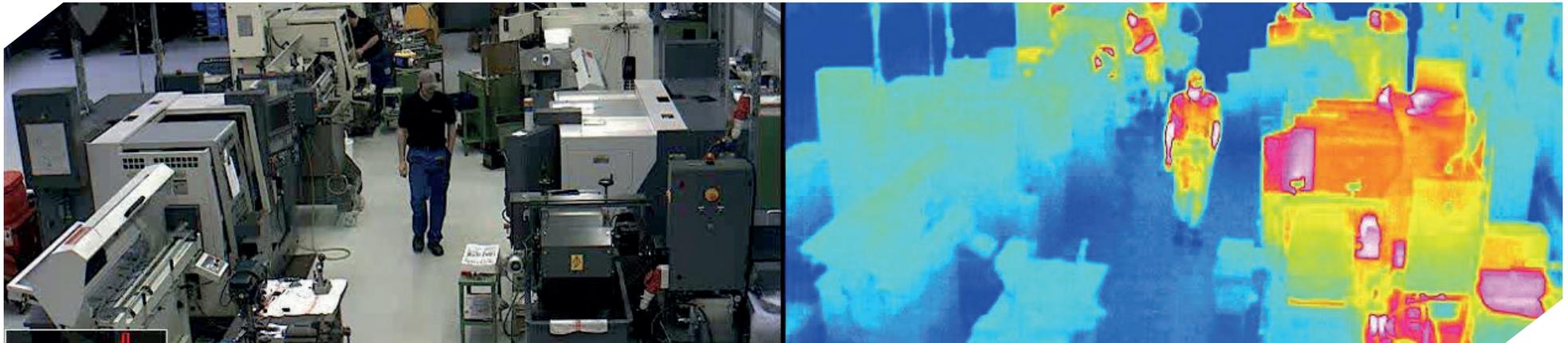
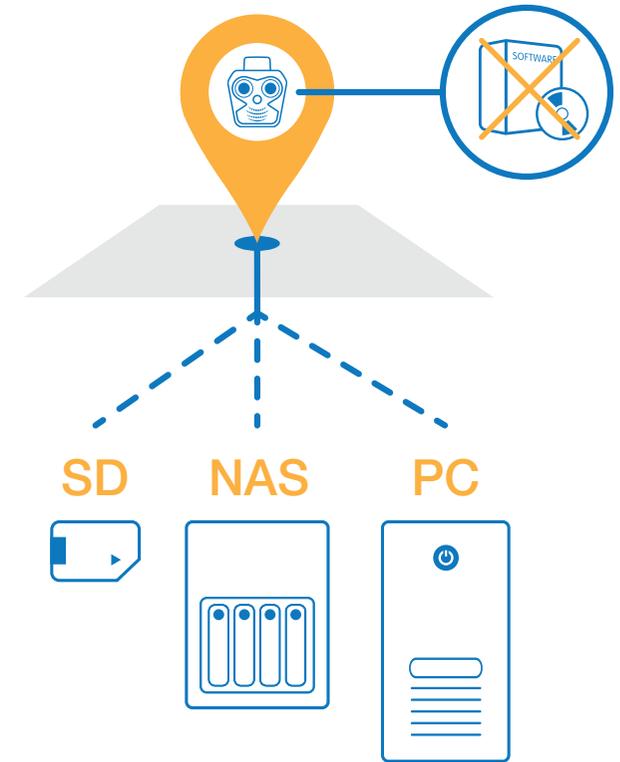
[Wikipédia](#)

La solution doit aussi être adaptable et interopérable, c'est-à-dire :

- **S'intégrer à un système existant**, numérique et/ou analogique, et dans un CSV
- **Être ouverte et sécurisée sur d'autres traitements sur l'image** : reconnaissance de plaques d'immatriculation, reconnaissance faciale, détection de mouvement, ou encore chute de corps
- **Être ouverte et sécurisée sur d'autres modules IOT** (Internet des objets connectés) : portail électrique, alarmes, détecteurs luminosité, humidité, gaz, mouvements, chaleur, ou encore vibrations

Cette approche permet de :

- Améliorer la redondance
- Réduire les besoins en bande passante, donc réduire la consommation d'énergie
- Faire évoluer la mémoire interne ou externe en fonction des besoins
- Réduire les coûts de gestion des enregistrements liés aux licences logicielles



6/ Comment garantir la protection de mes données et se prémunir des cyberattaques ?

Les systèmes de vidéosurveillance étant des objets connectés à un réseau d'entreprise, ils constituent une porte d'entrée potentielle pour les pirates. Alors, afin de protéger les données et de se prémunir contre les cyberattaques, il est nécessaire d'adopter une approche de protection globale comprenant :



- **Un chiffrement de bout en bout** pour toutes les données relatives aux images source, au système de gestion d'image, mais aussi les données stockées, pour se protéger des logiciels malveillants.
- **Une sécurité « dès la conception »** avec un développement logiciel qui ne délivre pas ses technologies afin de limiter l'exposition aux incidents de sécurité de matériels tiers.
- **Un système d'authentification** au logiciel de gestion des vidéos construit pour supprimer les risques de vulnérabilité et d'intrusion, notamment grâce à un hachage des mots de passe utilisateurs.
- **Un chiffrement vidéo** réalisé directement au sein de la caméra afin d'assurer un très haut niveau de sécurité et d'intégrité des données.
- **Un serveur web intégré** à la caméra sécurisé grâce à la détection et l'interdiction de toute exécution de scripts externes, c'est-à-dire des attaques sur les mots de passe.



Certification. Les produits certifiés par le Centre National de Prévention et de Protection (CNPP) ont une garantie supplémentaire de fiabilité, de résistance, et de sécurité, notamment aux cyberattaques.

L'intégrité assure que les données ne subissent aucune altération ou destruction volontaire ou accidentelle, et qu'elles conservent un format permettant leur utilisation tout au long de leur vie. [Centre National de Prévention et de Protection \(CNPP\)](#)

7/ Comment maximiser son Retour Sur Investissement (ROI) ?

Si les solutions « low cost » ne sont pas recommandées, il est néanmoins possible de faire l'acquisition d'un système de vidéo-protection à faible coût et fournissant un fort ROI. Et ce grâce à une solution comprenant :

- **Une sécurité intégrée** : les caméras intègrent l'analyse vidéo

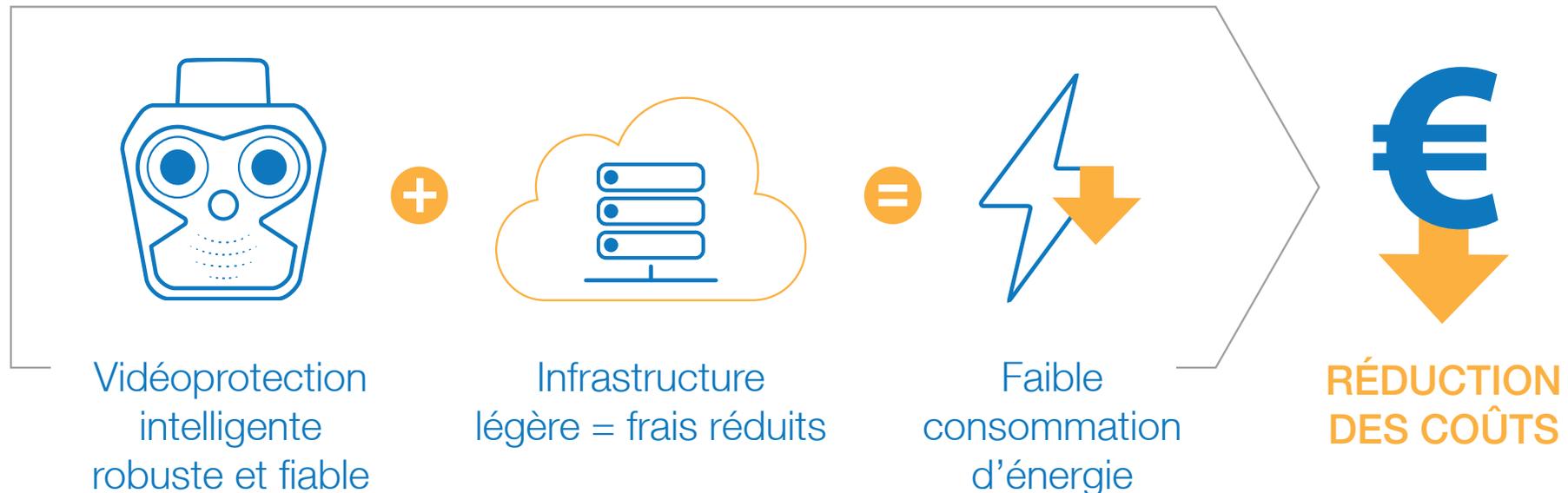
- **De l'intelligence intégrée** : lorsque les caméras intègrent directement l'intelligence et l'analyse vidéo, il n'y a pas de frais de gestion de serveur et ceux pour le stockage des données est significativement réduit.

- **Du matériel fiable** : avec des caméras robustes et fiables, les coûts de remplace-

ment de matériel et de maintenance sont considérablement réduits.

Par ailleurs, avec ce type de solution, les économies d'énergie sont importantes.

DES COÛTS FAIBLES POUR UN ROI ÉLEVÉ



Conclusion

Les caméras ne doivent pas être de simples équipements mais des objets connectés, qui, grâce à des technologies intelligentes, cybersécurisées, et déployées sur des systèmes décentralisés – donc extrêmement performants et énergétiquement sobres – protègent les personnes et les biens matériels. Ce sont alors bien plus que des caméras, mais des plateformes, qui proposent une solution complète adaptée aux usages de chaque entreprise, et qui vont bien au-delà de la vision humaine.





KONICA MINOLTA

**Konica Minolta
Business Solutions France**

365-367 route de Saint-Germain
78424 Carrières-sur-Seine Cedex
www.konicaminolta.fr

S.A.S au capital de 29 365 200 Euros
RCS Versailles B302 695 614

Retrouvez toutes nos solutions sur www.digital-solutions.konicaminolta.fr