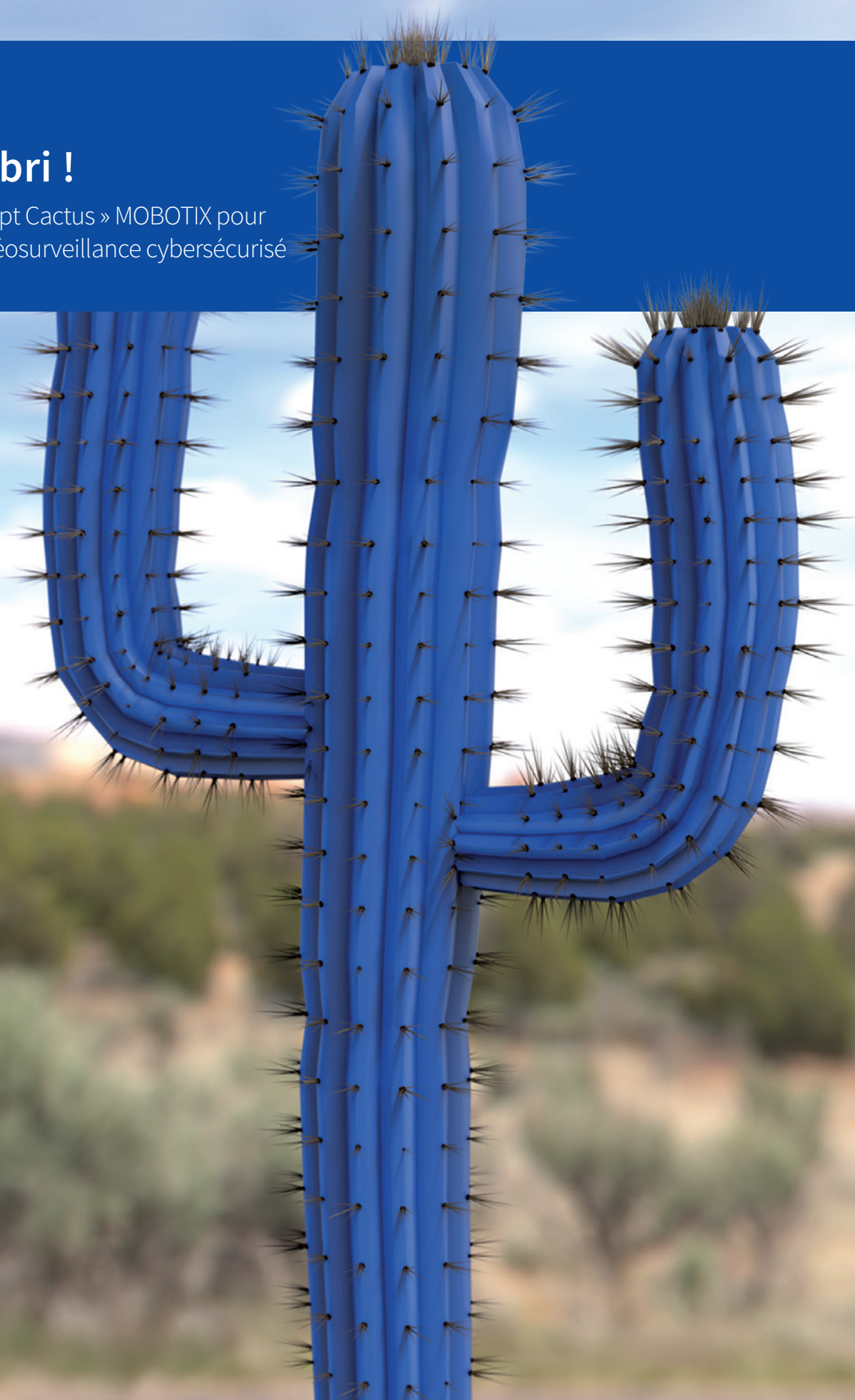


Restez à l'abri !

Découvrez le « Concept Cactus » MOBOTIX pour
votre système de vidéosurveillance cybersécurisé





Introduction – Qui est MOBOTIX ?

MOBOTIX est un développeur et fabricant de systèmes de contrôle d'accès et de vidéo IP de haute sécurité allant au-delà de la vision humaine. MOBOTIX se focalise sur la sécurité et Concept Cactus avec sa technologie intelligente décentralisée innovante, qui combine des données visuelles, thermiques, sonores et de capteurs afin de mieux protéger chaque environnement.

Conçues pour une utilisation intuitive assistée par une intelligence artificielle, les solutions MOBOTIX aident à résoudre les problèmes les plus épineux dans les domaines du commerce de détail, de l'éducation, de la santé, des transports, de la mobilité et des lieux d'hébergement. L'équipement MOBOTIX est conçu sans pièces mobiles et inclut des contrôles de cybersécurité à la pointe du secteur afin de fournir le meilleur retour sur investissement possible. Une longue durée de vie

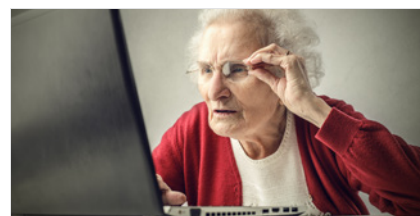
est garantie, qui est encore renforcée par des mises à jour logicielles continues.

Pourquoi la cybersécurité pour les systèmes de vidéosurveillance est-elle si importante ?

La vidéosurveillance pour la sûreté et la sécurité aide des milliards d'individus au quotidien. De la famille flânant dans un centre commercial sous l'oeil vigilant d'une caméra de surveillance, au parents inquiets surveillant le sommeil de leur bébé, la vidéosurveillance est présente dans chaque aspect de notre vie. Plus d'un million de caméras MOBOTIX ont été installées dans le monde grâce à un réseau de partenaires certifiés présents dans 150 pays.

Avec tous ces avantages, les systèmes de vidéosurveillance sont devenus une cible potentielle des attaques criminelles. Dans le passé, les attaques contre les réseaux de

vidéosurveillance étaient rares en raison de la nature privée des transmissions filaires en boucle entre les sites surveillés et les 3 salles de contrôle. Les temps ont changé et, désormais, les caméras vidéo modernes sont des ordinateurs exécutant des logiciels connectés à une caméra vidéo. L'usage croissant d'Internet et de caméras à faible coût a facilité l'accessibilité aux systèmes de vidéosurveillance via les réseaux IP, ce qui a entraîné une augmentation des risques de cyberattaque.



Risques des cyberattaques :

- Le nombre croissant d'appareils IP crée davantage de cibles
- Désactivation et contrôle à distance
- Collecte de données
- Prise de contrôle et détournement d'appareils
- Espionnage industriel et commandité par les gouvernements

Dégâts potentiels

Les cyberattaques réussies contre les systèmes de vidéosurveillance et de contrôle d'accès peuvent mener à des pertes humaines et à d'autres dégâts importants par le biais d'attaques criminelles ciblées et plus efficaces. De plus, alors que les systèmes de vidéosurveillance sont de plus en plus souvent obligatoires pour certains établissements autorisés à vendre des boissons alcoolisées ou dans le cadre d'une couverture d'assurance, si un système de vidéosurveillance devient inopérant en raison d'une cyberattaque évitable et qu'un délit est commis et non enregistré par la caméra, les assureurs peuvent refuser une réclamation à cause d'un manquement aux conditions d'application des garanties.



Dégâts potentiels :

- Pertes financières et atteinte à la réputation
- Mesures réglementaires, amendes et poursuites pour négligence
- Ruptures de contrats, réclamations pour dommages
- Pertes humaines à cause d'attaques terroristes ciblées

La protection des réseaux de vidéosurveillance soulève aussi la question du respect de la vie privée. La plupart des gouvernements imposent désormais que

toutes les données à caractère personnel relatives à la santé, aux finances, aux opinions politiques et à divers autres aspects soient conservées dans des conditions optimales de sécurité. Cette obligation s'applique également aux données vidéo. Par exemple, les enregistrements vidéo d'un individu assistant à un rassemblement politique doivent être conservés en sécurité et hors du domaine public. En cas de cyberattaque contre un dispositif ou un réseau de vidéosurveillance, il existe un risque très élevé que des informations privées telles que des images et autres données permettant de retrouver des personnes en particulier soient volées puis diffusées sans autorisation. Ceci porterait atteinte aux droits des utilisateurs à la protection de la vie privée par l'intermédiaire du système et pourrait entraîner des poursuites légales à l'encontre de la personne responsable du traitement des données personnelles.

Dans tous ces domaines, si la négligence peut être prouvée, cela peut déboucher sur une grave atteinte à la réputation, l'application de mesures réglementaires, des amendes et des poursuites pénales. En matière civile, ces situations peuvent également être synonymes de rupture de contrat, de poursuites et de recours collectif.

Position du secteur

Les dispositifs de contrôle d'accès et de vidéosurveillance font partie des technologies dites de l'Internet des objets (IoT, « Internet of Things »). Les entreprises et

analystes technologiques tels que Gartner et Cisco estiment que jusqu'à 50 milliards d'appareils IoT seront en usage d'ici 2020 (source : www.cisco.com). Contrairement aux transmetteurs radio, aux chaînes de télévision et aux véhicules à moteur, il n'existe pratiquement pas de législation relative aux objets connectés à Internet. Il n'existe pas de norme de sécurité obligatoire concernant la sécurité d'un objet, et avec le développement des applications autonomes, le risque que des appareils non sécurisés soient le siège d'attaques virales comme ce fut le cas des ordinateurs de bureau pourrait réapparaître sur des dispositifs tels que les réseaux de caméras de vidéosurveillance, pour lesquels il existe peu de moyens de détecter le problème ou de remédier rapidement à la situation.



Attaque du botnet « Mirai », 2016

Caméras IP affectées pour la première fois

Exemples de serveurs endommagés :

9/2016 Minecraft, OHV

10/2016 Dyn

11/2016 (élections présidentielles américaines) : Twitter, Spotify, Amazon

11/2016 Gouvernement libérien

11/2016 Deutsche Telekom

Incident concret

Souvent, les cyberattaques contre les dispositifs de vidéosurveillance ne sont pas

détectées ni signalées. Lorsque ces dispositifs sont détournés puis utilisés pour attaquer d'autres ressources Internet, il est toutefois difficile d'ignorer le problème. Une attaque massive de ce type, due en partie à un réseau de dispositifs de vidéo-

surveillance détournés par une cyberattaque, a affecté Twitter, Amazon, Tumblr, Reddit, Spotify et Netflix à l'automne 2016. Le botnet était essentiellement constitué de caméras IP et d'enregistreurs vidéo numériques (DVR) fabriqués par une

société chinoise de haute technologie. Les composants fabriqués approvisionnent les fournisseurs grand public et se retrouvent par dizaines de milliers dans leurs produits, pouvant devenir des cybermenaces potentielles.

Découvrez le « Concept Cactus » MOBOTIX

Pour faire face à ces problèmes, MOBOTIX a créé une stratégie de cybersécurité appelée « Concept Cactus », visant à fournir une approche globale pour la protection des produits MOBOTIX contre la menace des cyberattaques.

Le cactus symbolise l'idée au cœur de la stratégie de cybersécurité de MOBOTIX : chaque composant matériel et logiciel est protégé par une panoplie d'éléments défensifs afin de stopper les menaces extérieures.

Par exemple, tel un cactus protégé par ses épines et sa peau dure, MOBOTIX utilise un chiffrement de bout en bout sans aucun

angle mort, de l'image source au système de gestion d'image installé sur l'ordinateur de l'utilisateur en passant par les câbles de données et le stockage de données. A l'instar d'un cactus dont les branches sont recouvertes d'épines, tous ces modules, incluant la caméra, le stockage, les câbles et le système de gestion vidéo du système MOBOTIX, possèdent des épines numériques qui les protègent de tout accès non autorisé.

Toutefois, les technologies de sécurité ne sont efficaces que si le processus à disposition de l'utilisateur pour exploiter ces systèmes l'est également. De ce fait, le « Concept Cactus » prévoit également de

sensibiliser les clients existants et potentiels de MOBOTIX sur la question de la sécurité des données dans les systèmes de vidéosurveillance en réseau et de les informer sur les solutions économiques et efficaces qui peuvent protéger les organisations.

Les éléments du Cactus Concept

L'entreprise MOBOTIX fait figure d'exception au sein du secteur car elle développe son propre logiciel en interne et ne délivre pas de licence pour ses technologies à des parties tierces. Cette approche innovante apporte des avantages significatifs en matière de sécurité. En contrôlant la chaîne complète de développement logiciel, MOBOTIX est moins exposée aux incidents de sécurité résultant de logiciels et de matériel tiers qui ont affecté d'autres marques. Le Concept Cactus est fidèle à l'esprit de « sécurité dès la conception » présent depuis les débuts de l'entreprise, et chaque domaine le prouve.



Le cactus :

Croît dans des environnements hostiles

Très économique

Très robuste

Longue durée de vie

Protégé par des épines



Logiciel et développement sécurisés

L'approche de MOBOTIX pour la sécurité s'exprime dès la conception du système d'exploitation et des couches applicatives. Tous les appareils MOBOTIX sont construits sur un système d'exploitation Linux modifié et sécurisé qui supprime les services et modules standards. Les modules Linux critiques, tels que l'authentification, sont entièrement recréés par les ingénieurs MOBOTIX afin d'éliminer les risques de vulnérabilité aux intrusions et aux techniques d'injection de code classiques. Ce logiciel d'exploitation, qui n'est pas open source, est protégé par des procédures de sécurité supplémentaires. En outre, chaque mise à jour du micrologiciel de l'appareil et des composants logiciels est chiffrée et signée numériquement pour éviter les tentatives d'altération.

Sécurité des appareils et de la communication

Tous les enregistrements générés par la caméra sont chiffrés en interne, en commençant par la mémoire tampon circulaire qui utilise la carte SD intégrée dans chaque caméra. MOBOTIX a développé un

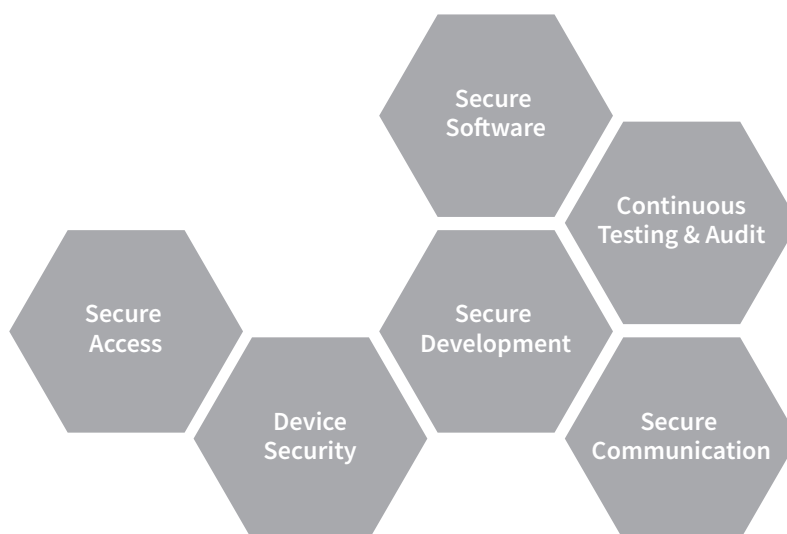
système de fichiers sécurisés grâce auquel, si une caméra est volée ou piratée, les vidéos enregistrées et encore présentes dans l'appareil ne peuvent pas être récupérées sans avoir obtenu au préalable les droits d'administrateur, eux-mêmes protégés par les processus de sécurisation de la configuration décrits précédemment. Chaque appareil MOBOTIX peut également être équipé de mécanismes contre le vol et l'altération tels que des boîtiers renforcés, capteurs, alarmes et fonctions d'alerte.

L'accès à l'interface de configuration de la caméra n'est octroyé qu'aux utilisateurs autorisés. Par mesure de sécurité, la création et l'application de privilèges différents par groupe d'utilisateurs relève d'un processus interne à chaque système. En pratique, les mots de passe utilisateur ne sont jamais enregistrés en clair dans les caméras MOBOTIX, mais sont hachés grâce à un algorithme de hachage unidi-

rectionnel puissant (SHA-512). Même si le fichier de configuration tombait entre de mauvaises mains, la récupération du mot



de passe en clair s'avèrerait quasiment impossible. Les services non essentiels sont désactivés pour limiter les intrusions potentielles et prévenir les attaques, et il n'existe aucun « mot de passe maître » non documenté. La seule manière d'accéder à une caméra MOBOTIX et de la configurer est via son interface utilisateur graphique (GUI) Web.



Restez à l'abri avec MOBOTIX

La popularité de la vidéosurveillance est en hausse et les menaces de cyberattaques aussi. MOBOTIX protège activement ses appareils contre ces risques et notre Cactus Concept a pour but de sensibiliser les clients existants et potentiels de MOBOTIX sur la question cruciale de la sécurité des données dans les systèmes de vidéosurveillance en réseau.

En fournissant les outils nécessaires à la création d'environnements plus sécurisés pour nos clients et grâce à notre engagement pour faire de la sécurité un élément fondamental de la proposition de valeur de MOBOTIX, nous continuerons à coopérer avec nos pairs, nos clients et les services gouvernementaux afin de protéger les technologies et les systèmes essentiels qui contribuent à rendre la société plus sûre pour chacun d'entre nous. Rendez-vous sur la page Concept Cactus de notre site web pour plus d'information :

Rendez-vous sur la page Concept Cactus de notre site web pour plus d'information :

www.cactusconcept.com

MOBOTIX

[Solutions](#)[Produits](#)[Support](#)[Société](#)[Partenaires](#)

[Newsroom](#)[Sélecteur de produits](#)[Trouver un partenaire](#)[Login Partner Section](#)[Langue](#)

The MOBOTIX Cactus Concept

Stay Untouched.



Connaissez-vous les avantages d'une solution de vidéosurveillance en réseau intégrant un concept cactus pour l'ensemble de votre matériel et de vos logiciels?

Cela vous semble onéreux ? Pas d'inquiétude. Personne ne souhaite investir une somme trop importante dans des dispositifs de sécurité, et personne n'en a l'obligation. Nous vivons malheureusement dans un monde où les individus recherchent la bonne solution vidéo et sous-estiment l'importance de la fiabilité du système. Et ils finissent par en payer le prix. Aujourd'hui, pour se protéger des cyberattaques toujours plus nombreuses menées par des pirates informatiques dans le monde entier, plus aucun système n'est fiable sans un concept de protection complet et adapté.

Chez MOBOTIX, nous avons développé un concept unique du cactus qui offre aux systèmes vidéo complets une protection totale et fiable contre les cyberattaques. Protégez-vous des futures attaques à chaque fois que quelqu'un essaie de transformer votre solide environnement informatique en champ de ruines. Armez-vous contre une attaque de grande ampleur en faisant l'acquisition d'un système vidéo intelligent prêt à l'emploi capable de relayer les défis en constante évolution de notre monde. Chaque jour. Sans surcoût.

Les systèmes vidéo MOBOTIX comptent parmi les plus sûrs au monde. Basés sur un extraordinaire concept technologique décentralisé, ils offrent par défaut de nombreuses mesures de protection contre les cyberattaques. Découvrez ce qui se cache derrière le concept cactus de MOBOTIX et ce qu'un système de vidéosurveillance totalement sécurisé peut vous apporter.

[Guide de cyberprotection](#)

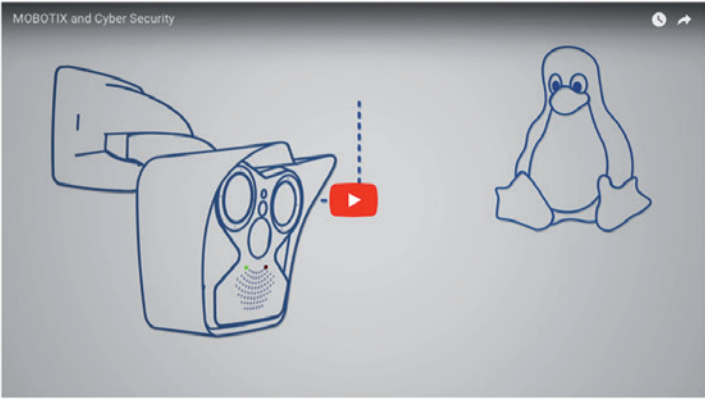
Le livre blanc de la cybersécurité

Les cyberattaques contre les dispositifs et infrastructures de vidéosurveillance ne cessent d'augmenter. Dans ce livre blanc informatif, vous découvrirez comment MOBOTIX est devenue leader de l'industrie dans ce combat contre cette tendance inquiétante et apprendrez les bonnes pratiques permettant de construire un environnement d'exploitation plus solide et sûr.

Pour recevoir le lien de téléchargement par e-mail, il vous suffit de remplir le formulaire.

Gardez vos équipements MOBOTIX à jour et téléchargez les derniers micrologiciels et logiciels.

[Download](#)



En savoir plus sur le concept cactus de MOBOTIX

Objectif du concept cactus	>
Sécurité de bout en bout	>
Une conception durable sans pièces mobiles	>
Un dispositif incroyablement économe et ne nécessitant que peu de maintenance	>
Résistance aux intempéries et aux températures élevée	>
Incrediblement utile	>
Un concept complet impressionnant	>
Une évolution, pas une révolution	>

6

Beyond Human Vision

Notre USP n'est pas une entité individuelle, ni un élément de conception unique.

Chez MOBOTIX, notre USP correspond à un pack technologique innovant et de qualité, conçu pour fournir une solution complète. Nous combinons chaque élément pour offrir la plus

grande flexibilité et un ensemble d'outils haute technologie, qui vous permettent de résoudre des problèmes concrets de la manière la plus efficace et la plus fiable possible.

Avec MOBOTIX, nous allons au-delà de la vision humaine, afin de vous aider aujourd'hui tout en vous préparant pour l'avenir !



FR_01/19

MOBOTIX AG

Kaiserstrasse
D-67722 Langmeil
Tel.: +49 6302 9816-103
Fax: +49 6302 9816-190
www.mobotix.com

Distribué par :

