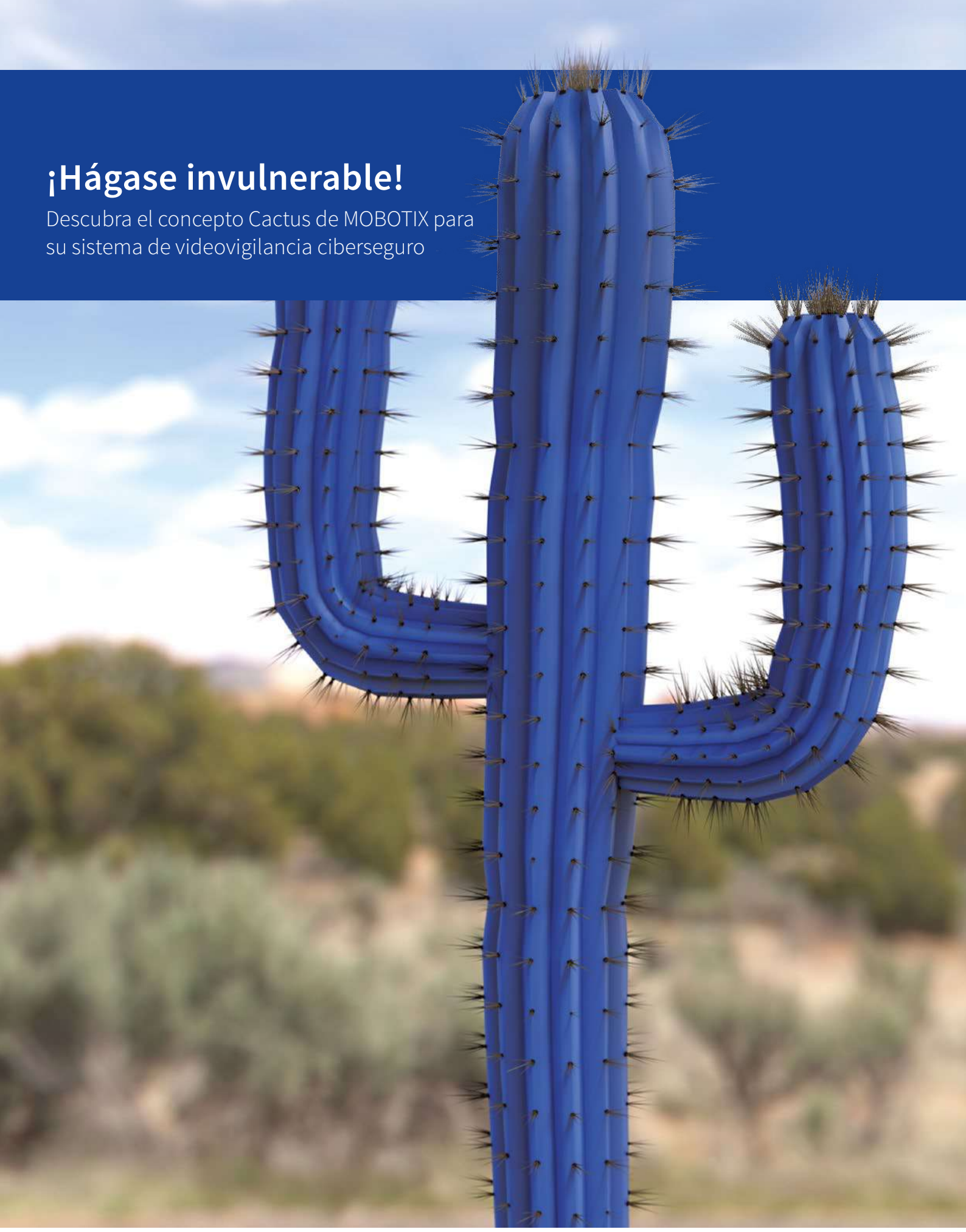
¡Hágase invulnerable!

Descubra el concepto Cactus de MOBOTIX para su sistema de videovigilancia ciberseguro



BeyondHumanVision

MOBOTIX

Presentación: ¿Quiénes somos?

MOBOTIX es un desarrollador y fabricante de sistemas de vídeo IP y de control de acceso de alta seguridad bajo el lema “Beyond Human Vision” (más allá de la visión humana). MOBOTIX, con su atención centrada en la seguridad y más allá de esta, es una empresa pionera en la tecnología descentralizada inteligente que combina datos visuales, térmicos, sonoros y de sensores para proteger mejor cualquier entorno.

Diseñadas para un funcionamiento intuitivo y asistido mediante inteligencia artificial, las soluciones de MOBOTIX ayudan a resolver los mayores retos de los sectores de venta al por menor, educativo, sanitario, de transporte, movilidad y hostelería. Los equipos MOBOTIX están diseñados sin piezas móviles y cuentan con elementos de control de ciberseguridad líderes en el sector a fin de proporcionar el mejor retorno de inversión global. Cuenta con una larga vida operativa garantizada que mejora aún más mediante continuas actualizaciones de software.

¿Por qué es tan importante la ciberseguridad en los sistemas de videovigilancia?

La videovigilancia garantiza la seguridad y esta, por su parte, ayuda a miles de millones de personas todos los días. Desde una familia que pasea por un centro comercial seguro bajo la atenta mirada de una cámara de videovigilancia hasta unos padres preocupados por monitorizar a un bebé dormido, la videovigilancia afecta a todos los aspectos de nuestras vidas. De hecho, se han instalado más de un millón de cámaras MOBOTIX en todo el mundo a través de una red de partners certificados que se extiende por 150 países.

Con todos estos beneficios, los sistemas de videovigilancia se han convertido en un objetivo potencial de los ataques de delincuentes. Hasta ahora, los ataques contra las redes de videovigilancia eran poco frecuentes debido a la naturaleza cerrada de los sistemas, que a menudo se conectaban mediante redes privadas cableadas directamente a las salas de control in situ. Sin embargo, los tiempos cambian y las cámaras de vídeo actuales son, de hecho, pequeños ordenadores que ejecutan software conectados a una cámara de vídeo. Con el auge de Internet y las cámaras de bajo coste, los sistemas de videovigilancia son cada vez más accesibles a través de cualquier red IP, lo que conlleva el aumento de ciberataques potenciales.

Riesgos de ciberataques:

- El creciente número de dispositivos IP implica más objetivos
- Desactivación y control remoto
- Recopilación de datos
- Control y uso indebido de los dispositivos
- Espionaje industrial y con autorización gubernamental
- Acceso bloqueado por ataques

Posibles daños

Los ciberataques que consiguen dañar los sistemas de videovigilancia y de control de acceso pueden ocasionar la pérdida de vidas e importantes daños materiales mediante ataques criminales realizados de manera selectiva y con mayor éxito. Además, dado que los sistemas de videovigilancia son obligatorios para cada vez más instalaciones autorizadas o como parte de coberturas de seguro, si un sistema de videovigilancia se vuelve inoperativo debido a un ciberataque evitable y se comete un delito, pero no se captura en cámara, las aseguradoras pueden negarse a satisfacer cualquier reclamación debido al incumplimiento de las condiciones de la cobertura.

Posibles daños:

- Pérdidas financieras y daños de imagen
- Medidas normativas, multas y enjuiciamiento por negligencia
- Incumplimientos de contrato, reclamaciones de daños y perjuicios
- Pérdida de vidas humanas a través de ataques terroristas selectivos

La protección de las redes de videovigilancia también plantea problemas de privacidad personal. La mayoría de los gobiernos exige actualmente que todos los datos personales privados sobre salud, finanzas, afiliación política y una serie de criterios adicionales se guarden de manera segura. Esto también se aplica a datos de vídeo; por ejemplo, las personas que asisten a eventos políticos esperan que todas las imágenes de videovigilancia se conserven de forma segura y fuera del dominio público. En el caso de un ciberataque contra un dispositivo o red de videovigilancia, existe un riesgo muy elevado de que la información personal, como imágenes y otros datos, se pueda relacionar con determinadas personas y pueda ser robada y filtrada sin autorización. Esto supondría una violación de los derechos de privacidad de los usuarios monitorizados por el sistema y podría tener consecuencias legales para el responsable del procesamiento de datos personales.

En todas estas áreas, si se puede probar la negligencia, existe la posibilidad de daños de imagen considerables, medidas disciplinarias, multas y procesos penales. En asuntos civiles, esto también podría dar origen a demandas por incumplimiento de contrato, tanto individuales como colectivas.

Postura de la industria

Los dispositivos de videovigilancia y de control de acceso pertenecen al tipo de tecnologías denominado Internet de las cosas (IoT, Internet of Things). Las empresas de tecnología y los analistas como Gartner y Cisco, entre otros, prevén que para 2020 existan 50 000 millones de dispositivos IoT en funcionamiento (fuente: www.cisco.com). A diferencia de los transmisores de radio, las emisoras de televisión o los vehículos de motor, apenas existe legislación sobre lo que se puede conectar a Internet. No hay estándares obligatorios sobre el nivel de seguridad que debe ofrecer un dispositivo, y a medida que la tecnología se vuelve más autónoma, existe el riesgo de que los dispositivos no seguros atraigan virus como las epidemias que solían inundar los ordenadores de escritorio, que podrían reaparecer en dispositivos como las redes de cámaras de videovigilancia, para las que no existen muchas formas de detectar o de solucionar rápidamente el problema.

Ataque de botnet «Mirai», 2016
Primera vez que las cámaras IP resultan afectadas

Ejemplos de servidores dañados:

9/2016	Minecraft, OHV
10/2016	Dyn
11/2016	(campaña elecciones presidenciales EE. UU.): Twitter, Spotify, Amazon
11/2016	Gobierno de Libia
11/2016	Deutsche Telekom

Incidente real

Los ataques cibernéticos contra dispositivos de videovigilancia no se suelen detectar ni notificar. Sin embargo, cuando se toma el control sobre estos dispositivos y posteriormente se utilizan para atacar otros recursos de Internet, los problemas son más difíciles de ignorar. En otoño de 2016 se produjo un ataque a gran escala que afectó a Twitter, Amazon, Tumblr, Reddit, Spotify y Netflix y que fue provocado, en parte, por una red de dispositivos de videovigilancia que había sido objeto de un ciberataque. La botnet está compuesta principalmente por grabadoras de vídeo digital (DVR) y cámaras IP fabricadas

por una empresa china de alta tecnología. Los componentes que se fabrican se venden a proveedores que posteriormente los utilizan en sus propios productos, lo que conlleva que varias decenas de miles se hayan incorporado a estas peligrosas armas cibernéticas.

Presentación del concepto Cactus de MOBOTIX

En respuesta a estos problemas, MOBOTIX ha creado la estrategia de ciberseguridad llamada „Concepto Cactus“ que tiene como objetivo ofrecer una solución integral para proteger los productos MOBOTIX frente a la amenaza de los ciberataques.

El cactus simboliza la idea central subyacente en la estrategia de ciberseguridad de MOBOTIX donde cada componente de hardware y software está protegido por un conjunto de defensas que bloquean las amenazas externas.

Por ejemplo, al igual que las espinas y la gruesa capa exterior del cactus, MOBOTIX utiliza cifrado de extremo a extremo sin puntos ciegos desde la fuente de la imagen, pasando por los cables de datos y el almacenamiento de datos, hasta el sistema de gestión de vídeo en el equipo del usuario. Al igual que un cactus, cuyas ramas están cubiertas de espinas, todos los módulos del sistema MOBOTIX (cámara, almacenamiento, cables y sistema de gestión de vídeo) cuentan con espinas digitales que los protegen de accesos no autorizados.

No obstante, las tecnologías de seguridad sólo son tan buenas como lo sean los procesos que utilice el usuario para manejar estos sistemas. Así pues, otro objetivo del concepto Cactus es el de concienciar a los clientes actuales y potenciales de MOBOTIX sobre la importancia de la seguridad de los datos en los sistemas de videovigilancia basados en red y mostrarles de qué forma las organizaciones se pueden proteger a sí mismas mediante soluciones rentables e inteligentes.

Elementos del concepto Cactus

MOBOTIX sigue unos procesos poco habituales en su sector ya que desarrolla todo su software de forma interna y no concede licencias de su tecnología a terceros. Este enfoque innovador ofrece un beneficio significativo en lo que respecta a la seguridad. Al controlar la cadena completa de desarrollo del software, MOBOTIX es menos vulnerable a los puntos débiles de terceros que han afectado a otras marcas en casos en los que una vulnerabilidad de un componente de software o hardware de terceros conduce a un problema de seguridad. El concepto Cactus sigue una ética de seguridad a través del diseño que forma parte de la empresa desde el primer día y que resulta evidente en todas las áreas.

El Cactus:

Crece en entornos difíciles

Muy austero

Muy robusto

Tiene una larga vida

Se protege mediante espinas

Software y desarrollo seguros

El enfoque de seguridad de MOBOTIX comienza con el diseño del sistema operativo y la pila de aplicaciones. Todos los dispositivos MOBOTIX se diseñan sobre un sistema operativo Linux modificado y protegido que elimina los servicios y módulos estándar. En su lugar, los módulos de Linux críticos, como la autenticación, son completamente rediseñados por los ingenieros de MOBOTIX para garantizar que

no ofrecen vulnerabilidades estándar ni están expuestos a técnicas de inyección de código. Este software operativo no es de código abierto y está protegido por técnicas de seguridad de software adicionales. Además, cada actualización del firmware del dispositivo y de los elementos del software se cifra y firma digitalmente para evitar su manipulación.

Seguridad de los dispositivos y las comunicaciones

Todas las grabaciones registradas por la cámara se cifran internamente, lo que comienza por el búfer circular que utiliza la tarjeta SD incluida en cada cámara. MOBOTIX ha construido un sistema de archivos seguro mediante el cual, si se piratea o roba una cámara, el vídeo grabado que aún se encuentra en la cámara no se puede recuperar sin antes obtener derechos de administrador, que están protegidos mediante los procesos de configuración segura descritos anteriormente. Todos los dispositivos MOBOTIX se pueden equipar también con mecanismos antirrobo y antimanipulación, que incluyen carcasas reforzadas, sensores, alarmas y funciones de alerta.

Sólo los usuarios autorizados pueden acceder a la interfaz de configuración de la cámara y, para garantizar la seguridad interna, todos los sistemas permiten la creación y aplicación de diferentes derechos para grupos de usuarios distintos. En la práctica, esto significa que las cámaras MOBOTIX nunca guardan las contraseñas de los usuarios en formato de texto no cifrado, sino que se crean con un avanzado algoritmo de cifrado unidireccional (SHA-512) para que, incluso si el archivo de configuración termina en malas manos, sea extremadamente difícil recuperar el texto explícito de la contraseña. Los servicios no esenciales están desactivados, lo que limita las posibles vulnerabilidades y evita ataques. Además, no existe una «contraseña maestra» sin documentar: la única forma de acceder y configurar una cámara MOBOTIX es a través de su GUI (interfaz gráfica de usuario) web.

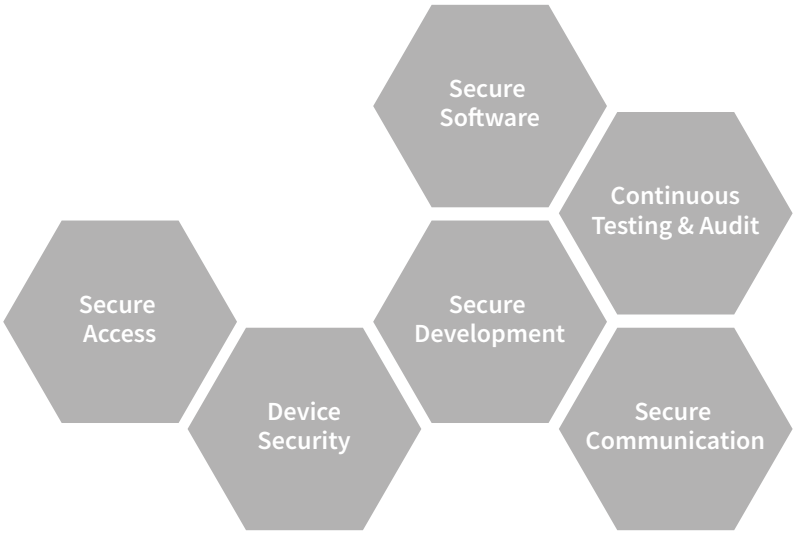
Comunicación segura de red y dispositivos

Todos los datos intercambiados entre cada cámara MOBOTIX y otros hosts de la red se pueden cifrar para garantizar la confidencialidad e integridad de los datos que se transmiten. La misma tecnología que se utiliza para asegurar sitios de banca por Internet HTTPS (SSL/TLS) y certificados digitales se incluye por defecto para cumplir con las mejores prácticas empleadas en los principales marcos de seguridad por expertos.

MOBOTIX también ofrece compatibilidad con la administración de certificados únicos X.509 en cada cámara y autoridades de certificados raíz para permitir a las organizaciones ampliar la seguridad de sus dispositivos a fin de incluir cámaras y videoporteros autenticados a través de sistemas como OpenVPN. Esto significa que, si se roba o piratea una cámara, un atacante no puede usar las credenciales que se encuentran en dicha cámara para atacar al resto de la red de cámaras.

Pruebas y auditorías continuas

Sin embargo, todas estas medidas se deben validar para ofrecer un entorno verdaderamente seguro. Para garantizar esto, MOBOTIX utiliza los servicios de SySS (www.syss.de), una prestigiosa empresa independiente de evaluación de seguridad que comprueba la seguridad tanto de los elementos de software como de hardware. Las pruebas incluyen pruebas de penetración completas por parte de equipos de hackers especializados que intentan acceder a nuestros elementos de control, lo que nos permite corregir cualquier vulnerabilidad antes de alcanzar la fase de producción.



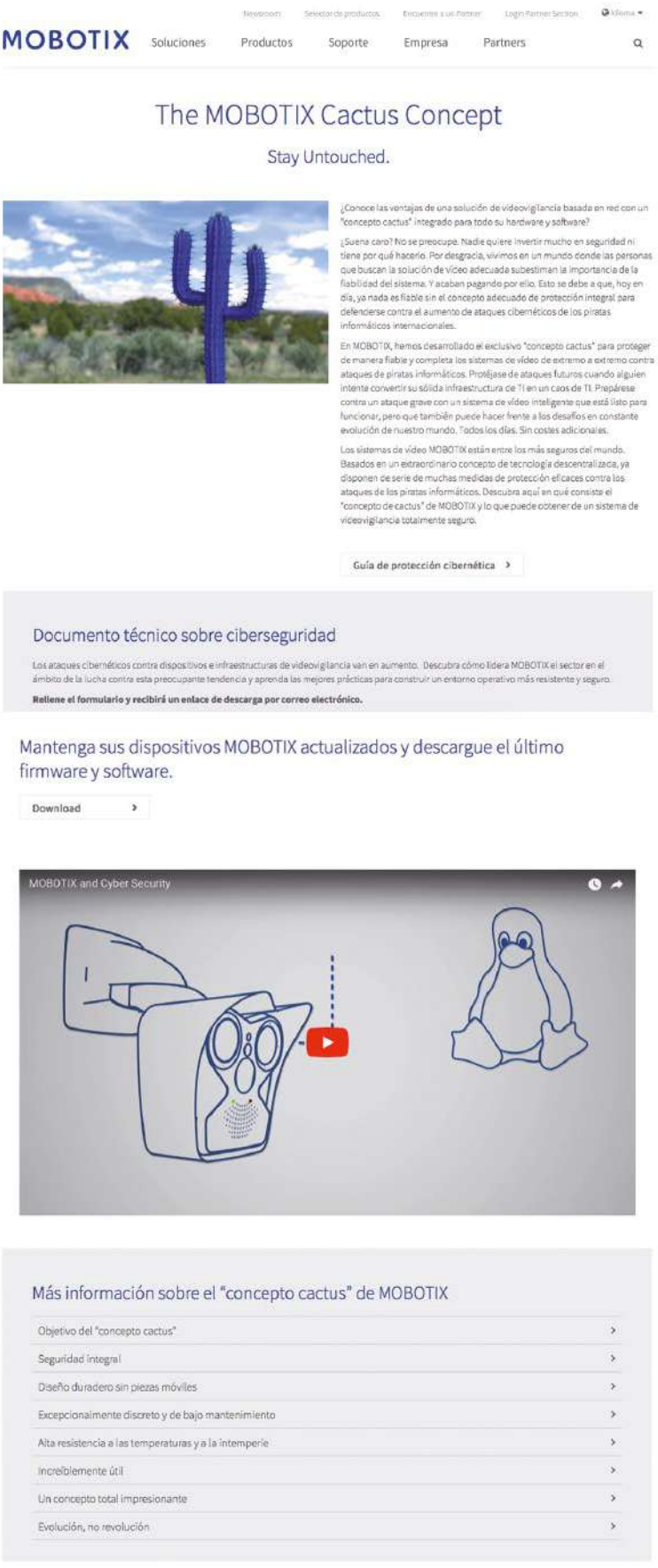
Hágase invulnerable con MOBOTIX

La popularidad de la videovigilancia está aumentando, al igual que las amenazas de ciberataques. MOBOTIX protege de forma activa sus dispositivos frente a posibles riesgos y el concepto Cactus tiene como objetivo concienciar a los clientes actuales y potenciales de MOBOTIX sobre el importantísimo problema de la seguridad de los datos en los sistemas de videovigilancia basados en red.

Al proporcionar las herramientas para ayudar a nuestros clientes a crear entornos más seguros junto con el compromiso de hacer de la seguridad una parte fundamental de la propuesta de valor de MOBOTIX, esperamos seguir trabajando con nuestros homólogos del sector, los clientes y los organismos gubernamentales para proteger todas esas tecnologías y sistemas que contribuyen a que la sociedad sea más segura para todos.

Visite nuestra página “Concepto Cactus” en el sitio web para obtener más información:

www.cactusconcept.com



BeyondHumanVision

Nuestra USP no es una sola función o un solo elemento de diseño.

La propuesta única de venta de MOBOTIX es el conjunto de tecnología, innovación y calidad diseñado para ofrecer una solución completa. Combinamos cada elemento para ofrecer la máxima flexibilidad junto con un juego de herramientas de alta ingeniería que le permite solucionar problemas del mundo real de la manera más eficiente y fiable.

En MOBOTIX vamos más allá de la visión humana para ayudarle hoy, ¡y prepararle para el futuro!

ES_04/18

MOBOTIX AG

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

MOBOTIX