Stay Untouched!

Discover the MOBOTIX Cactus Concept for your Cyber-Secured Video Security System

Distributed by

BeyondHumanVision

MOBOTIX

Introduction – Who Are MOBOTIX?

MOBOTIX is a developer and manufacturer of high-security IP video and access control systems that go Beyond Human Vision. Focused at and beyond security, MOBOTIX has pioneered intelligent decentralized technology combining visual, thermal, sound and sensor data to better protect every environment.

Designed for intuitive operation assisted by artificial intelligence, MOBOTIX solutions help solve the most challenging problems within retail, education, healthcare, transportation, mobility and hospitality sectors. MOBOTIX equipment is designed without moving parts and includes industry leading cyber security controls to provide the best overall return on investment. An extended operating lifetime is guaranteed and further enhanced by continual software upgrades.

Why is Cyber Security for Video Surveillance Systems so Important?

Video surveillance to ensure safety and security helps billions of people each day. From a family wandering around a safe shopping centre under the watchful eye of a video surveillance camera or concerned parents monitoring a sleeping baby; video surveillance touches all of our lives. In fact, over one million MOBOTIX cameras have been installed worldwide through a network of certified partners spanning 150 countries.

With all these benefits, video surveillance systems have become a potential target for attack by criminals. In the past, attacks against video surveillance networks were rare due to the closed nature of systems that would often link by private directly cabled networks to on-site control rooms.

However, times change and modern video cameras are effectively computers running software connected to a video camera. With the rise of the internet and lower cost cameras, video surveillance systems are increasingly accessible over any IP network which has led to the rise of potential cyber-attack.

Risks of Cyber-Attacks:

- Increasing numbers of IP devices creates more targets
- Deactivation and remote control
- Collecting data
- Takeover and misuse of devices
- Industrial and government-sponsored espionage
- Access blocked by ransomware attacks

Potential Damages

Successful cyber-attack against video surveillance and access control systems can lead to potential loss of life and other significant damage through targeted and more successful criminal attacks. In addition, as video surveillance systems are increasingly a mandate for certain licensed premises or as part of insurance coverage, if a video surveillance system is rendered inoperable due to a preventable cyber-attack and a crime is committed but not captured on camera – insurance providers may refuse to honour any claim due to failure to meet the terms of coverage.

Potential Damage:

- Financial losses and reputation damage
- Regulatory measures, fines and prosecution for negligence
- Breaches of contract, damage claims
- Loss of human life through targeted terrorist attacks

Protecting video surveillance networks also raises issues of personal privacy. Most governments now mandate that all private personal data across areas such as health, finance, political affiliation and a host of other criteria must be stored in a secure fashion. This also extends to video data – for example, an individual attending a political rally – expect any video surveillance footage to be kept secure and outside of the public domain. In case of a cyber-attack against a video surveillance device or network, there is a very high risk that the personal information such as images and other data that could track back to specific persons can be stolen and leaked without authorisation. This would violate the privacy rights of the users monitored by the system and could have legal consequences on the designated person responsible for processing personal data.

Across all these areas, if negligence can be proven, there is the potential for significant reputational damage, regulatory action, fines and criminal prosecutions. In civil matters, there is also the potential for breach of contract, civil and class action lawsuits.

Industry Position

Video surveillance and access control devices are part of a category of technologies called the Internet-of-Things (IoT). Technology firms and analysts such as Gartner, Cisco and others estimate up to 50 billion IoT devices will be in use by 2020 (Source: www.cisco.com). Unlike radio transmitters, TV stations or motor vehicles, there is almost no legislation around what can be attached to the internet. There are no mandated standards around how secure an item must be and as technology becomes more autonomous, there is a risk that unsecured devices will attract virus like epidemics that used to plague desktop computer users, and could start to reappear on devices like video surveillance camera networks for which there are few ways to either detect or quickly defeat the problem.

“Mirai” botnet attack, 2016
IP cameras affected for the first time

Examples of damaged servers:

9/2016	Minecraft, OHV
10/2016	Dyn
11/2016	(U.S. presidential election): Twitter, Spotify, Amazon
11/2016	Liberian Government
11/2016	Deutsche Telekom

Real World Incident

Cyber-attacks against video surveillance devices are often not detected or reported. However, when these devices are taken over and then used to attack other internet resources, the issues are harder to ignore. A massive such attack in autumn 2016 that impacted Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix was, in part, generated by a network of video surveillance devices that had been taken over by a cyber-attack. The botnet is mainly comprised of digital video recorders (DVRs) and IP cameras made by a Chinese hi-tech company. The components make are sold downstream to vendors who then use it in their own products leading to tens of thousands of co-opted into these dangerous cyber weapons.

Introducing The MOBOTIX Cactus Concept

In response to these issues, MOBOTIX has created a cyber security strategy called the "Cactus Concept" that aims to deliver a comprehensive approach to protecting MOBOTIX products against the threat of cyber-attacks.

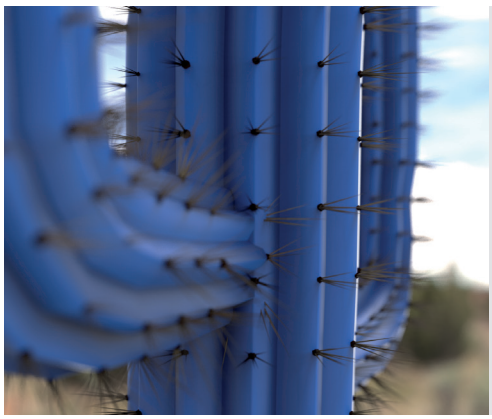
The cactus symbolizes the core idea behind the MOBOTIX cyber security strategy where every piece of hardware and software is protected by an array of defences to stop external threats.

For example, like the thorns and tough skin of the cactus, MOBOTIX uses end-to-end encryption with no blind spots from the image source via the data cables and the data storage through to the video management system on the user's computer. Like a cactus, whose every limb is covered in thorns, all of these modules including the camera, storage, cables and video management system in the MOBOTIX system have digital thorns that protect them from unauthorized access.

Yet security technologies are only as good as the process in place for the user to operate these systems. As such, another objective of the Cactus Concept is to raise awareness among potential and existing MOBOTIX customers of the importance of data security in network-based video security systems and how organizations can protect themselves through cost-efficient and intelligent solutions.

The Elements of the Cactus Concept

MOBOTIX is unusual within the industry as it develops all of its own software in-house and does not licence its technology to third parties. This innovative approach offers significant benefit when it comes to security. By controlling the entire chain of software development, MOBOTIX is less vulnerable to third party weaknesses that have impacted other brands where a vulnerability within a third party software component or hardware leads to a security problem.



The Cactus:

Grows in tough environments

Is very economical

Is very robust

Has very long lifespan

Is protected by thorns

The Cactus Concept is a "security by design ethos" that has been within the company from day one and this is evident every area.

CYBER SECURITY INITIATIVE

Secure Software and Development

The start of the MOBOTIX security approach begins within the design of the operating system and application stack. All MOBOTIX devices are built on top of a modified and secured Linux OS that removes standard services and modules. Instead, critical Linux modules like authentication are completely re-designed by engineers at MOBOTIX to ensure that these modules are not vulnerable to standard exploits or code injection techniques. This operating software is not open source and protected by additional software security techniques. In addition, every update to device firmware and software elements are encrypted and digitally signed to avoid tampering.

Device Security and Secure Communication

All the recordings generated by the camera are encrypted internally and this starts with the ring buffer that uses the built in SD card

in each camera. MOBOTIX has built a secure file system that means if a camera is physically hacked or stolen, previously recorded video still in the camera cannot be retrieved without first gaining administrator rights that are protected through the secure configuration processes as described previously. Each MOBOTIX device can also be fitted with anti-theft and anti-tamper mechanisms including reinforced housings, sensors, alarms and alert functions.

Access to the camera configuration interface is granted to only authorized users and to ensure internal security, every system allows the creation and enforcement of different rights for different user groups. In practice this means that MOBOTIX cameras never save user passwords in clear text but instead are hashed with a strong one-way hashing (SHA-512) algorithm so that even if the configuration file ends up in the wrong hands, it would be extremely difficult to retrieve the password in clear text. Unessential services are disabled to limit potential exploits and prevent attacks and there is no undocumented "master password" – the only way to access and configure a MOBOTIX camera is via its Web GUI (Graphical User Interface).

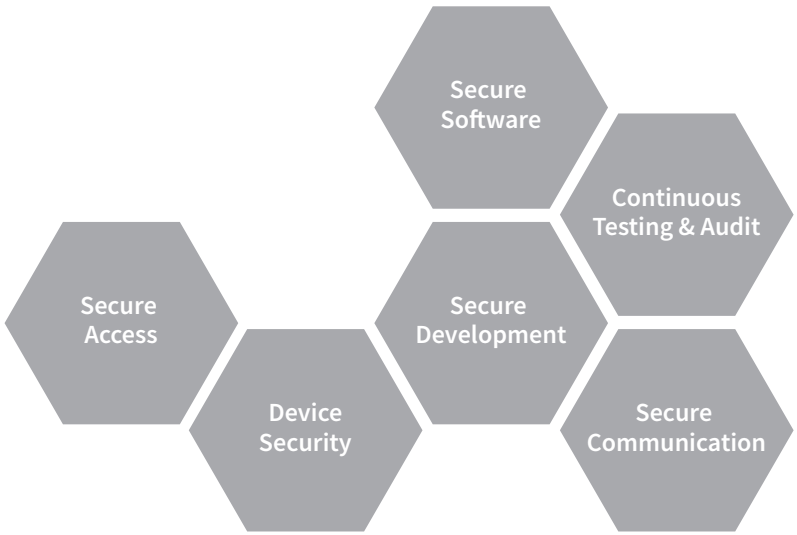
Secure Network and Device Communication

All data exchanged between every MOBOTIX camera and other hosts in the network can be encrypted to ensure confidentiality and integrity of data in transit. The same technology used to secure internet banking sites HTTPS (SSL/TLS) and digital certificates are all supported as standard to meet the best practice guidance that resides within the major security frameworks from experts.

MOBOTIX also includes built in support to manage unique X.509 certificates on each camera and Root Certificate Authorities to allow organisations to extend device security to include cameras and Door Station devices authenticated via systems like OpenVPN. This means that if a camera is physically stolen or hacked, an attacker cannot use the credentials within a compromised camera to attack the rest of the network of cameras.

Continuous Testing and Audit

Yet all of these measures need to be validated as delivering a truly secure environment. To ensure this, MOBOTIX uses the services of SySS (www.syss.de), a highly regarded and independent third party security testing company that examines the security of both software and hardware elements. The testing extends to full penetration testing using teams of specialist hackers that attempt to breach our controls – to allow us to fix any faults before they reach the production stage.



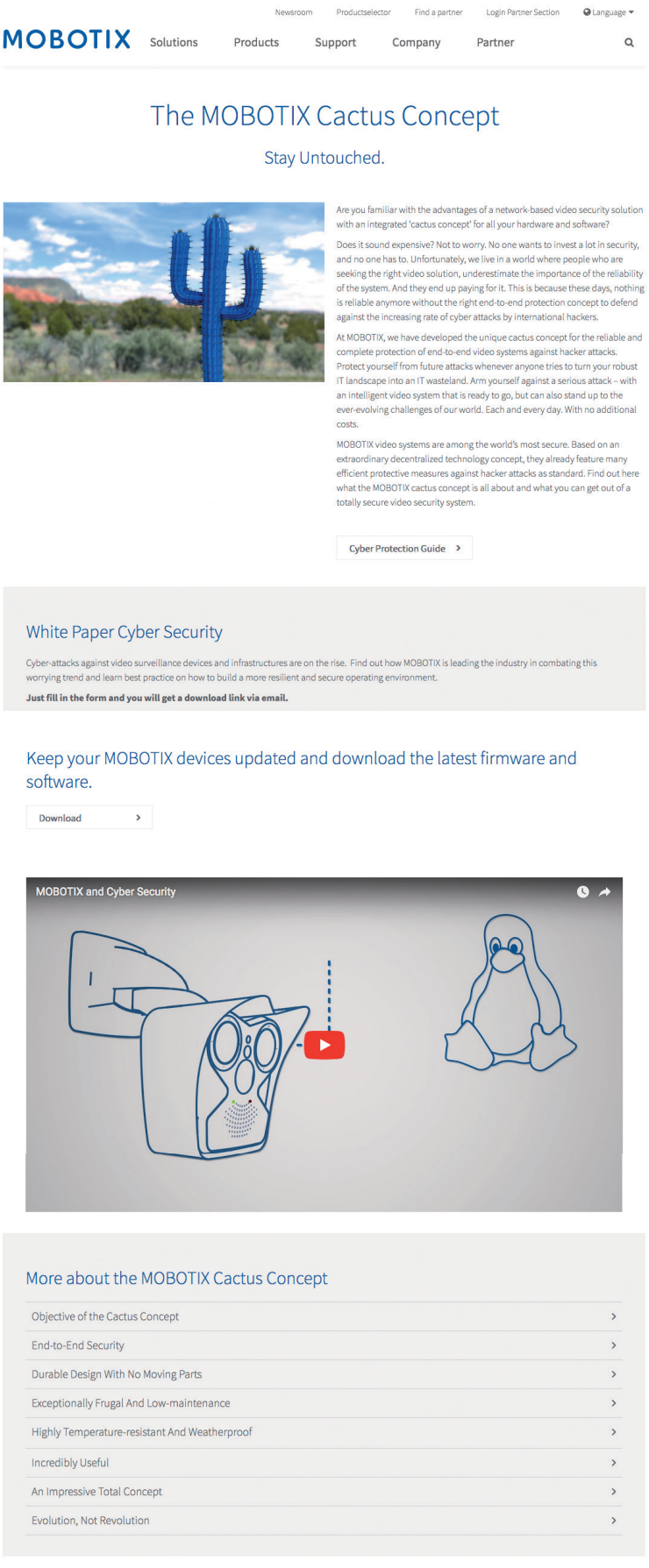
Stay Untouched with MOBOTIX

The popularity for video surveillance is rising as are the threats from cyber-attack. MOBOTIX is actively protecting its devices against the risks and our cactus concept aims to raise awareness among potential and existing MOBOTIX customers of the extremely important issue of data security in network-based video security systems.

By providing the tools to help our customers build more secure environments along with a commitment to making security a fundamental part of the MOBOTIX value proposition, we look forward to working with our peers in the industry, customers and government agencies to protect the very technologies and systems that help make society safer for all.

Visit our Cactus Concept page on the website for more information:

www.cactusconcept.com



Beyond Human Vision

Our USP is not an Individual Feature or a Single Design Element.

With MOBOTIX, our USP is the total package of technology, innovation and quality designed to offer a complete solution. We combine each element to offer the most flexibility along with highly engineered set of tools that allow you to solve real world problems in the most efficient and reliable manner.

With MOBOTIX, we go beyond human vision to help you today and prepare you for the future!

US_04/18

MOBOTIX CORP

80 Broad Street, Suite 702
New York, NY 10004
Tel.: +1 212 385 6126
www.mobotix.com

MOBOTIX