Arxan Application Protection for Medical Devices

Avoid a security emergency

Patient Safety is in the Hands of Medical Device Apps

People entrust their personal safety and lives to medical devices every day – from pacemakers and insulin pumps to hospital infusion pumps and other devices. However, medical devices are highly vulnerable to compromise because apps that drive the medical devices are insufficiently protected. One of the most prevalent medical device application security vulnerabilities is a lack of binary protection, which can allow for unauthorized access to critical controls and data. The risk is not hype – it's real. In July 2015, the US Food and Drug Administration (FDA) issued a warning about infusion pumps that were installed in more than 400,000 hospitals, which were discovered to be remotely hackable. Such devices could have been maliciously taken over to deliver lethal doses of medication to patients receiving IV drips. The security risks and safety hazards continue to escalate.

Top Medical Device Application Risks You Must Defend

- **Code Analysis:** Malicious actors can examine the medical device application code, either statically (for example, as dis assembled code) or dynamically (while the program is executing). Such analysis enables the adversary to understand how the internal algorithms work, discover sensitive information, and pinpoint vulnerabilities.

- **Intellectual Property (IP) Theft:** Attacks on medical device applications can be designed to extract sensitive information and steal copyrighted material or proprietary algorithms.

- **Cryptographic Key Theft:** Cryptographic keys are at the core of all security systems that deal with encrypted data. If hackers can locate keys in the code or medical device memory, they can completely circumvent or remove the security features and gain unauthorized access to the medical device.

- **Tampering:** Adversaries can install malicious code or modify controls, causing the program to malfunction, jeopardizing patient safety and compromising sensitive data.

- **Malware Injection:** Unprotected applications are exposed to malware insertion that can result in privacy breaches, performance loss, unauthorized remote control, and unintended medical device operation.

Arxan Protects Your Medical Device Apps so Patient Safety and Your Reputation are Assured

Arxan is the trusted leader in medical device application attack-prevention and self-protection. Arxan's solution empowers medical device manufacturers to protect the integrity of their device controls and confidentiality of sensitive data by:

- Blocking unauthorized access
- Preventing the copying, reverse-engineering, tampering, and modification of applications while stopping the insertion of malicious code

With the right combination of application code, cryptographic key, and data protection, medical device applications are safe from exposure and hacking.

Why Choose Arxan? Your Reputation is Everything.

Medical device customers appreciate the technical and business value our application protection delivers.

- **Security Strength:** multi-layer guard network delivers the most advanced application protection
- **Maturity:** we are protecting apps running on more than 500 million devices
- **Simplicity and Customizability:** integration is easy and security protection maps to your specific requirements
- **Service and Support:** world-class support from experts who are available when you need them
- **Trust and Stability:** financially strong company backed by top tier private equity firm; customers represent some of the world's leading brands

Arxan Automated Application Protection

DEFEND

Against reverse engineering, tampering and any manner of theft

DETECT

An attempted attack on the application code, or on another Guard

DETER

Attacks by safely exiting or silently deleting illegal assets or stealthily reporting back forensics information to a command center