medcrypt
Powered by Azure

PROACTIVE HEALTHCARE CYBERSECURITY - IN A FEW LINES OF CODE

MEDICAL DEVICE CYBERSECURITY SOLVED - EASY, ECONOMICAL, AND RELIABLE

Medical device manufacturers used to be able to ship a device, hope that there were no cybersecurity issues, and address problems as they were found. Today, with MedCrypt, leading device vendors proactively build security features into their devices before they ship, and win market share as a result.

THE BUSINESS CASE FOR CYBERSECURITY

CHALLENGE

Medical Device Manufacturers (MDMs) must decide how to transition from delivering innovative clinical solutions to also **delivering clinical solutions that are also secure**

RISK

MDM executives need to be aware of the risks and costs of doing security insufficiently or not at all. Insufficient cybersecurity measures can potentially impact:

RESPONSIBILITY

An MDM must be able to continue to focus on providing innovative clinical solutions, yet avoid passing security debt on to their customers by choosing to build or buy cybersecurity features.

SIMPLIFY

Developing security features is possible, but the costs can be significant and extend beyond the immediate development efforts. MDMs have conveyed to MedCrypt that after years of investment in internally developing security features, projects were dropped due to high development and maintenance costs.

HEALTHCARE FIRST CYBERSECURITY

VALUE

MedCrypt brings value to the MDM ecosystem with a set of **robust** and **ready-to-deploy** solutions that significantly **reduce the cost and effort** required to implement cybersecurity.

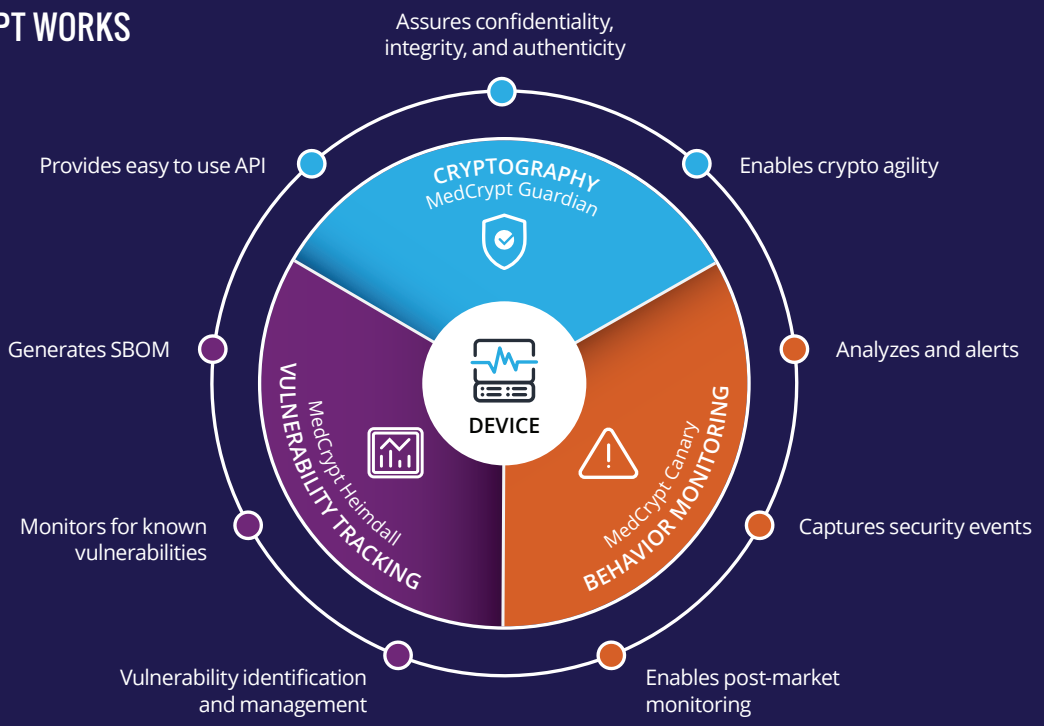
MedCrypt's software provides healthcare specific tools and API's to help make devices **secure by design**. These tools allow our customers to implement security features **easily and efficiently**, allowing MDMs to focus on delivering innovative clinical features.

By using MedCrypt, MDMs can get secure clinical features while reducing time to market, and meeting regulatory and customer cybersecurity requirements.

BENEFITS

- **Easy** and **cost-effective** implementation, operation, and maintenance
- Deterministic behavior, **scalable** across a wide range of architectures and platforms
- Assure **confidentiality**, **integrity**, and **authenticity** of device data, even in resource-restricted devices
- **Healthcare-specific** security behavior that meets unique medical device use cases
- **Securely** transmit device data independent of the integration environment
- Implement across the product development lifecycle, **supporting new and legacy designs**

HOW MEDCRYPT WORKS



MEDCRYPT GUARDIAN OVERVIEW

Each MedCrypt product addresses a specific set of security fundamentals, enabling medical device manufacturers to proactively, easily, and reliably protect critical information at rest and in transit, monitor devices for security events, and identify and manage device vulnerabilities.

In combination, these solutions enable manufacturers to not only protect critical device information and assure functional integrity, but also to holistically correlate security events with vulnerabilities and vice versa as well as identify affected versions and devices.

Cryptography

The **MedCrypt Guardian** library provides for easy implementation of common cryptographic functions to encrypt/decrypt and sign/verify data at rest or in motion.

- Provides easy to use API
- Enables crypto agility
- Assures confidentiality, integrity, and authenticity
- Optimized for the medical device use case
- Provision and manage unique device key pairs
- Customizable certificate infrastructure
- Wide platform support

MEDCRYPT USE CASE EXAMPLES

Use Case	Challenge presented to MedCrypt	Solution
Large-scale Capital Equipment	- Protect critical treatment and dosage data	- Sign/verify critical data flows
Remote Patient Care Ecosystem	- Protect data confidentiality across unprotected networks - Protect device configuration and functional integrity	- Encrypt data between device and remote service provider - Sign and verify firmware and configuration files uploaded to the device

Request a demo at info@medcrypt.com or visit us at www.medcrypt.com