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

Medical Device Manufacturers (MDMs) must decide how to transition from delivering innovative clinical solutions, to also delivering clinical solutions that are also secure. The impact of insufficient cybersecurity on the business has been well-documented. Beyond the risk to top line revenue, insufficient security can impact patient safety, the delivery of care, regulatory compliance, reputation, and legal exposure (including personal culpability for executives).

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. 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.

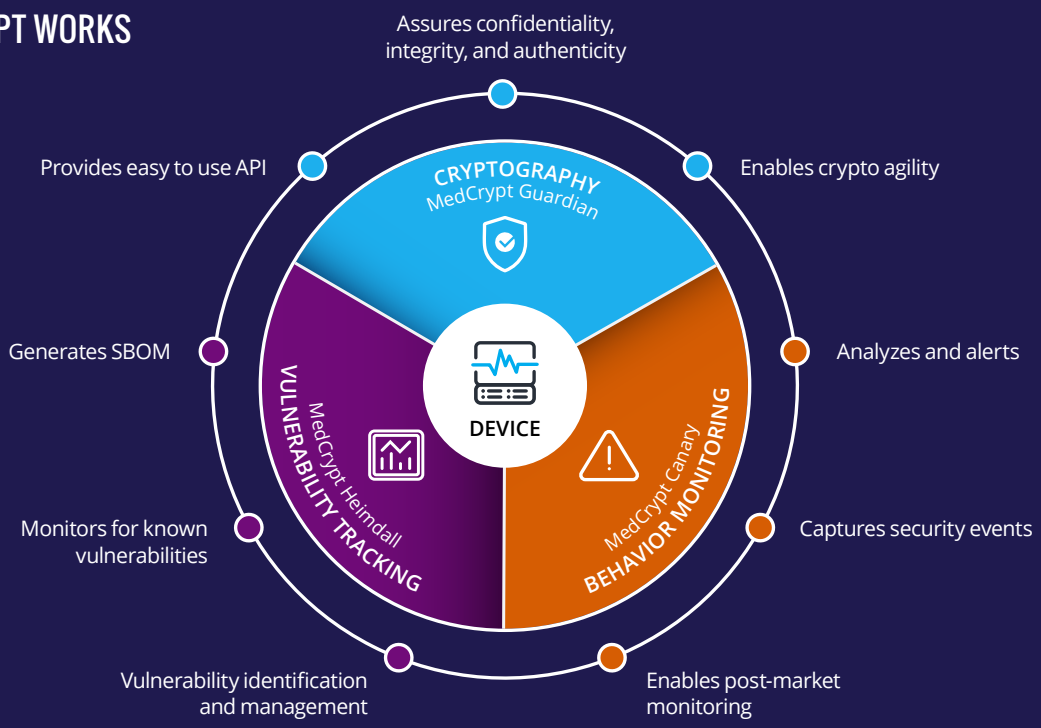
MDM executives need to be aware of the risks and costs of doing security insufficiently or not at all.

HEALTHCARE FIRST CYBERSECURITY

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.

- ☑ 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 PORTFOLIO 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

Behavior Monitoring

MedCrypt Canary is a remote monitoring tool that detects security events in deployed devices, filters out false positives, and informs mitigation strategies.

- Enables post-market monitoring
- Captures security event data and device metadata
- Analyzes and alerts
- Supports intermittent connectivity
- Can inform if a vulnerability has been exploited

Vulnerability Tracking

MedCrypt Heimdall extracts device SBOM, identifies and prioritizes vulnerabilities, and correlates exploited vulnerabilities across installed base to identify at-risk devices.

- Generates SBOM in multiple supported formats
- Monitors for known vulnerabilities (e.g., NVD) per SBOM version
- Tracks software libraries and dependencies across device platforms
- Reports identified vulnerabilities and affected devices
- Forensically links vulnerabilities to device events

MEDCRYPT USE CASE EXAMPLES

Use Case	Challenge presented to MedCrypt	Solution
Large-scale Capital Equipment	• Protect critical treatment and dosage data • Monitor for device security events • Enable postmarket management	**Guardian** **Canary** **Heimdall** • Sign/verify critical data flows • Detect signature verification failures • Identify and prioritize vulnerabilities
Bedside Monitoring and Life Supporting Equipment	• Need to maintain security posture of legacy device with unknown software structure	**Heimdall** • Extract SBOM, analyze software components for vulnerabilities, prioritize mitigation • On-going monitoring of current/updated
Remote Patient Care Ecosystem	• Protect data confidentiality across unprotected networks • Protect device configuration and functional integrity	**Guardian** • Encrypt data between device and remote service provider • Sign and verify firmware and configuration files uploaded to the device

MEDCRYPT HELPS MANUFACTURERS TO MEET FDA PRE - AND POST - MARKET REQUIREMENTS

1 Use Encryption

MedCrypt encrypts data at rest and in transit at the application layer, preventing data exposure and creating redundancy to unknown, unpredictable, and uncontrollable network security measures.

2 Use Digital Signatures

MedCrypt's embedded library allows users to sign code, data, instructions, configurations, etc. and verify these data structures before they are loaded into an active device.

3 Real Time Intrustion Detection

MedCrypt-enabled devices send behavior metadata (not PHI) to our telemetry system to monitor for suspicious behavior and security events. Healthcare-specific behavior baselines enable prioritization and reduction of false-positives.

4 Publish Device SBOM

MedCrypt enables multi-layer SBOM structural and component analysis, providing documentation required for regulatory filing. It matches components against identified vulnerabilities, enabling continual postmarket assessment and prioritized mitigation.

medcrypt

MedCrypt is a San Diego-based company that provides proactive security for healthcare technology. MedCrypt's platform brings core cybersecurity features to medical devices with just a few lines of code, ensuring devices are secure by design. MedCrypt announced a $5.3 million Series A funding round in May of 2019, bringing the total funds raised to $8.4 million with participation from Eniac Ventures, Section 32, Y Combinator, and more. The company is based in San Diego, California. For more, please visit www.medcrypt.com.

San Diego, California, USA
(877) MDC-RYPT (877-632-7978)
info@medcrypt.com | www.medcrypt.com