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 delivering innovative 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. The choice they must make is whether 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.

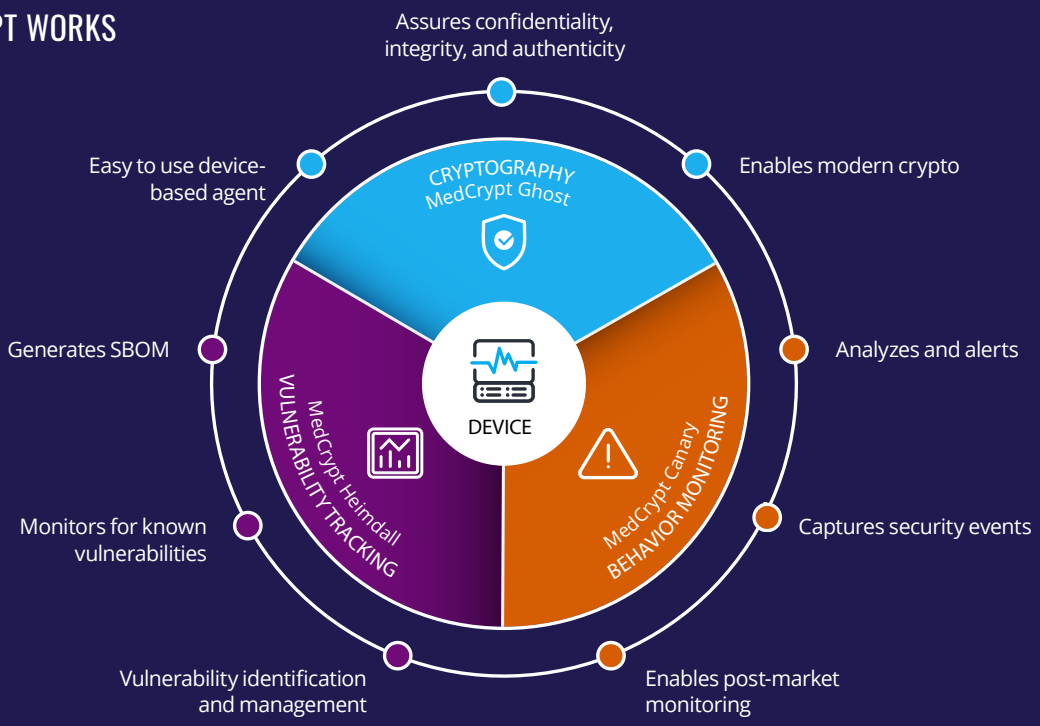
MDM executives need to be aware of the risks and costs of doing security insufficiently or not at all.

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 agents to help make both new and legacy 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 & 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 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 correlate security events & vulnerabilities while identifying affected versions and devices.

Cryptography

MedCrypt Ghost uses modern cryptography to secure data in transit with limited impact to the source code on your device.

- Easy to use agent that runs on a device
- Secure the transport layer communication on connected applications
- Automated key provisioning
- Provision and manage unique device key pairs over device lifetime
- Wide platform support

Behavior Monitoring

MedCrypt Canary is a remote monitoring agent 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 (no PHI)
- Analyzes and alerts
- Supports intermittent connectivity
- Informs if a vulnerability has been exploited

Vulnerability Tracking

MedCrypt Heimdall extracts the device SBOM, identifies and prioritizes vulnerabilities, and enables determining if a vulnerability has been exploited.

- Generates SBOM in multiple supported formats
- Monitors for known vulnerabilities (e.g., NVD) per SBOM version
- Tracks dependencies across device platforms
- Identifies 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 post-market management	**Ghost** **Canary** **Heimdall** • Secure critical data flows • Detect annomalous device behavior • 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 dependencies for vulnerabilities, prioritize mitigation • On-going monitoring of SBOM against widely used vulnerability sources
Interoperability	• Protect data confidentiality across devices on the same network • Protect functional integrity	**Ghost** • Securely communicate data between devices supported by different manufacturers • Implement modern cryptography

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

1 Use Encryption

MedCrypt encrypts data in transit, preventing data exposure and creating redundancy to unknown, unpredictable, and uncontrollable network security measures.

2 Key Management

MedCrypt delivers key management and configuration in an on-device agent, allowing for automated provisioning with little effort and maintenance over the lifetime of a 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 post-market assessment and prioritized mitigation.

medcrypt

MedCrypt provides proactive security for healthcare technology. MedCrypt's platform brings core cybersecurity features to medical devices, with little impact to source 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 $9.4 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