Guardian: Medical Device Cryptography Solution

Built-in security — not bolted on.

Guardian takes the complexity out of cryptographic security, handling key generation, secure storage, PKI, CA, and enforcement — so you don't have to.

From securing device-to-device communication to ensuring compliance, Guardian embeds security from Day 1. With seamless integration and automated lifecycle management, it simplifies encryption, mitigates risk, and lets you focus on innovation — not cryptography.

THE CHALLENGE

Stricter regulations

Evolving FDA cybersecurity requirements place full responsibility on MDMs.

Implementation barriers

Limited manufacturing connectivity and outdated security practices hinder adoption

Scalability & cost

Homegrown crypto is expensive, difficult to maintain, & lacks medical device alignment.

Innovation tradeoffs

Security integration competes with clinical feature development.

THE GUARDIAN SOLUTION

Seamless integration

From securing device-to-device communication to ensuring compliance, Guardian embeds security from day one with automated lifecycle management.

Root of Trust mechanisms

Stay resilient against emerging security challenges with continuous updates and evolution, offering long-term protection for your device subsystems.

Trusted key management

Establish secure connections with trusted keys for inter-device, server, or cloud communication with minimal implementation effort.

North-south protection

Secures device-to-cloud communication over any network. Supports uni/bidirectional traffic across multiple transport technologies.

East-west protection

Secures communication between device components. Integrates with protocols like DDS for enhanced local security.

Regulatory compliance

Provides authentication between endpoints and secure transit with unique keys, meeting FDA requirements and simplifying compliance.

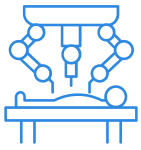
Who Should Use Guardian?

Guardian was built with medical device manufacturers in mind.

Devices with limited or no connectivity

Devices with limited memory & footprint

Complex system architectures



How Guardian Works

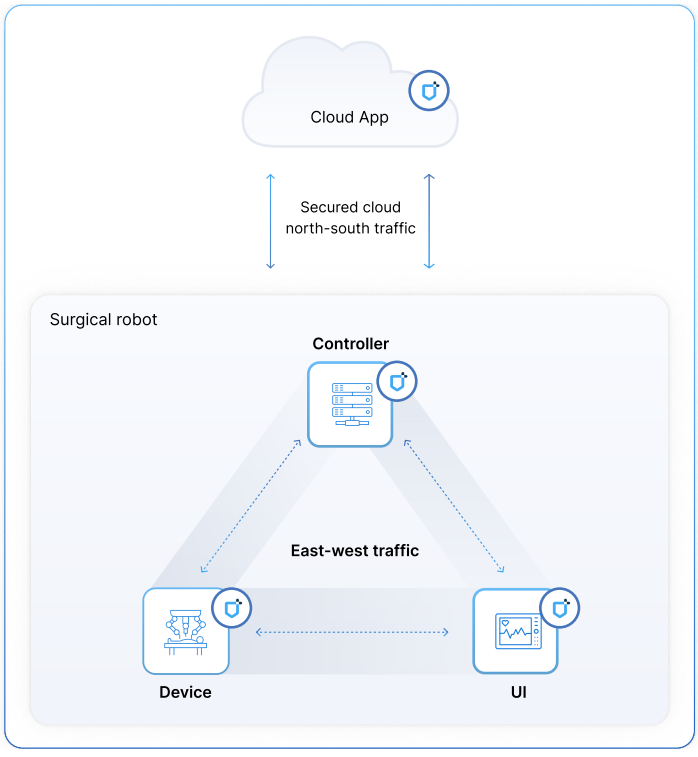
Guardian seamlessly integrates into your device ecosystem, automating cryptographic key management, secure storage, and enforcement. With built-in PKI and Certificate Authority (CA), it ensures encryption is correctly applied and maintained throughout the device lifecycle — eliminating complexity while meeting regulatory requirements.

↑↓ North-south protection (Device-to-cloud)

Secure communication between devices and cloud platforms over any network. Supports both unidirectional and bidirectional traffic across various transport technologies.

← → East-west protection (Local network)

Secures communication between device components with encryption & authentication. Seamlessly integrates with protocols like DDS to enhance local network security.



Guardian Platform: Purpose-built for medical devices

Ensuring the **highest level of cybersecurity** from development to market deployment.

> Our device was manufactured by a third party in an offline facility where keys were managed manually. Medcrypt provided a **scalable solution** to enable offline provisioning and lifecycle certificate management. Medcrypt's **familiarity with medical device manufacturing, engineering and regulatory environments** is why we **trust them for all our future cybersecurity needs**.
>
> Director of Product Security, Multinational MDM

Build vs Buy

Building security for the future is hard...if you're still trying to catch up to the present.
Get ahead before you're left behind.

CRITERIA	WHEN TO BUILD	WHEN TO BUY
Development time & speed to market	Tooling is unavailable and you have flexible timelines, with at least a year to build.	You have firm FDA submission dates with no flexibility in submission timelines.
FDA compliance	Your security team has the expertise, skills, and training to build an FDA-compliant solution that is secure-by-design.	Tooling satisfies the exact feature set recommended by the FDA
Quality documentation	You need to create and maintain QMS cybersecurity documentation that meets new guidances.	Solution includes support documentation that fulfills FDA requirements.
Expertise & resources	You have or can hire dedicated experts to handle the development, implementation, and ongoing maintenance.	Includes cybersecurity and engineering subject matter experts
Estimated 5-year cost to secure 1 product	**~ $22.8M**	**~ $11.8M**
Estimated time to secure 1 product	**~ 1 to 1.5 years**	**~ 8 weeks**