QNX

Foundational Cybersecurity for your Medical Device

The power to build trust



Introduction

Imagine that without warning a patient monitor goes dark. Not because of any patient status changes, but because the device has been compromised. In early 2025, CISA and the FDA flagged a patient monitor used in the USA and Europe that had a hidden backdoor and a critical, remotely exploitable flaw, one that could allow code execution and leak patient data. When a connected medical device fails in this way, the care and trust we all depend on for our family members and ourselves is compromised.

A compromised system and the resultant loss of trust is also a business concern. Today's medical devices are more connected and software-defined than ever, and every connection, component, and update is something a medical device manufacturer must choose and design carefully, while planning support for the entire life of the device.

Healthcare organizations face persistent cyber threats and, according to IBM's 2025 Cost of a Data Breach Report, healthcare continued to have the highest average cost per breach ($7.42M USD per breach) among the industries studied.

Cybersecurity vulnerabilities have a wide impact: patient and operator safety, downtime that disrupts patient care, loss of trust, damaged reputations, and the potential for significant financial loss.

Today's connected medical devices facilitate clinical tasks that once depended on human judgment alone, from interpreting imaging data to governing the delivery of therapy. This makes the performance of the foundational device software inseparable from patient safety. When a medical device cannot guarantee predictable behavior, fault tolerance, or withstand security events, the consequences reach beyond engineering into clinical, and business, risk. This is why the choice of a software foundation has moved from a technical preference to a strategic decision for the life of the medical device.

QNX is designed to serve as that foundation, and it already does for nine out of ten top medical device manufacturers. It is a secure, deterministic, real-time operating system with pre-certified safety technology, backed by experienced QNX Engineering Services and long-term maintenance options.

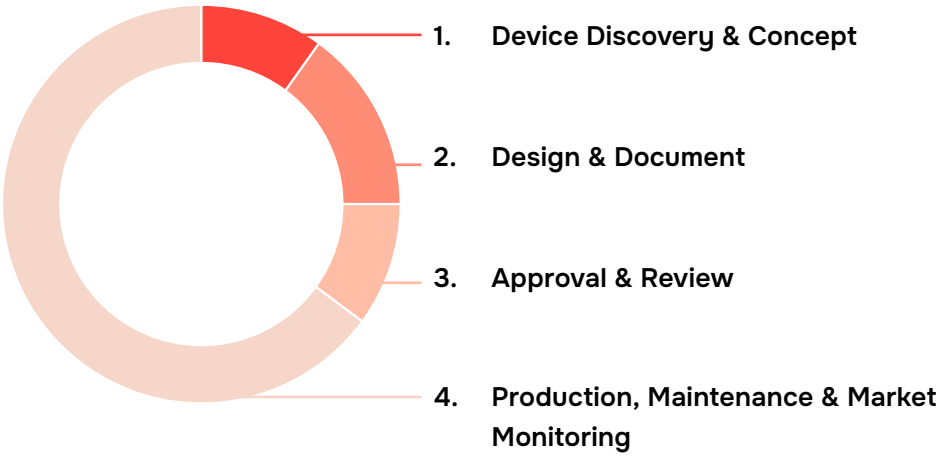
This brief illustrates how QNX is not only a secure foundation for real-time medical systems but also a strategic choice for all phases of your product lifecycle.

QNX & Cybersecurity Across the Product Lifecycle

The sections that follow are organized around four lifecycle phases, adapted from the FDA's Device Development Process, to show where QNX strengthens cybersecurity at each stage.

Typical example:

Relative time spent in medical product lifecycle



1. Device Discovery & Concept

This is the early development phase where architectural decisions and commitments will have a large effect later on costs and risks. Cybersecurity and threat modelling should be built in from the beginning to ease friction later in the process. QNX enables your teams to begin here with ease. The QNX Everywhere and Launchpad programs readily enable access to the secure production grade QNX platform for learning experimentation, and commercial prototyping respectively.

QNX uses a microkernel architecture which minimizes the amount of privileged code and contains faults to individual components versus a monolithic kernel design. By keeping software components separated from each other, attack vectors are isolated. This also constrains how far any compromises can reach, strengthening the cybersecurity posture of the software.

Committing to these controlled component separation boundaries at this early stage helps teams avoid costly security or safety redesign later when requirements and design harden. The QNX based high-performance cyber-resilient platform explored at this stage is the same real-time foundation that can later be shipped in a commercial product.

The transition from concept to commercial readiness becomes a licensing change using the same secure QNX architecture and is not a re-engineering exercise.

2. Design & Document

As the concept becomes a tested design, security decisions start to set in place. This is the best time to harden the device, because changes made now cost far less than changes made after a submission is in progress. Since the QNX foundation carries forward unchanged from the early prototypes, teams can spend this phase on the security of their own application rather than on reworking the base layer. That includes switching off services the device doesn't need, giving each component only the access it requires, and making sure only trusted software runs at startup.

The microkernel design also makes the security architecture easier to explain. Each driver, network stack and application runs in its own protected space, so the boundaries between components are clear. Teams can document those boundaries and the threat model as they build, which gives regulators the security architecture views they expect and saves last minute updates before submission.

Where deeper expertise is useful, QNX Engineering Services can advise or work alongside your engineers. The team brings decades of experience delivering safety-critical systems in highly regulated, security-critical industries.

3. Approval & Review

IEC 62304 is an internationally recognized software lifecycle standard commonly used to support the development and regulatory assessment of medical-device software. QNX OS for Safety (QOS) is independently pre-certified to IEC 62304 Class C by TÜV Rheinland. The QNX OS for Safety portfolio of pre-certifications includes not only IEC 62304 for medical, but also IEC 61508 SIL 3 for industrial, and ISO 26262 ASIL D and ISO/SAE 21434 for automotive. Across these demanding industries, QNX has a 100% success rate in achieving safety certification.

If a device meets the FDA definition of a cyber device, its premarket submission must comply with Section 524B of the FD&C Act. The FDA expects the medical device manufacturer to provide a cybersecurity management plan, proof of processes to give reasonable assurance of cybersecurity and a Software Bill Of Materials (SBOM). QNX provides ongoing vulnerability monitoring, assessment and remediation as part of our secure processes, which are key components in the cybersecurity management plan that the manufacturer provides. Additionally, QOS is provided with an SBOM that is regularly updated. All of this informs the cybersecure posture for the device and provides the software traceability and lifecycle support that simplifies the assessment and management of Off-The-Shelf (OTS) software that the regulatory authorities also expect to see. This helps manufacturers assess the impact of any vulnerabilities and maintain cybersecurity throughout the device lifecycle.

And because QOS is pre-certified to Class C and provided with accompanying documentation, a medical device manufacturer can focus its regulatory submission activity around its own application, rather than re-justifying the safety of the underlying foundational software. Simply put, the pre-certified QOS and associated safety artifacts provide usable evidence for the foundational operating system.

Ultimately the manufacturer remains responsible for demonstrating the safety of the complete medical device; however, using QNX helps provide that needed evidence for submission and lowers the efforts required to build the security strategies and safety cases. This reduces the documentation burden for the OS layer, which the FDA expects manufacturers to address as OTS software in their submission.

4. Production, Maintenance & Market Monitoring

While getting a medical device out to market is a significant achievement, the manufacturer's obligations do not end with regulatory approval and market access. Those ongoing responsibilities effectively begin and will continue for as long as the device remains in supported clinical use.

The design of the modular microkernel architecture that QNX uses supports the reality of long-term device maintenance and support. The modular aspect supports controlled, isolated updates that can be applied to individual components in a manner consistent with regulatory change-control expectations.

For required cybersecurity vigilance planning and monitoring, QNX has a dedicated Product Cybersecurity Team that tracks emerging vulnerabilities, newly disclosed CVEs (Common Vulnerabilities and Exposures), and any shifts in the overall threat landscape.

QNX product teams then provide regular remediation updates for QNX supplied components. These services enable device manufacturers to respond to issues in a timely, structured way and sustain cyber-resilience over the long-term. All while saving engineering hours for continued product portfolio innovations and predictably controlling total cost of ownership over the complete product lifecycle.

Conclusion: A Secure Lifecycle Strategy, Not Just an Operating System

Every phase of the device lifecycle traces back to decisions made at the start. A QNX microkernel foundation that isolates services, contains faults and behaves deterministically gives manufacturers a known path to cybersecurity, functional safety and regulatory readiness, while keeping the associated costs more controlled and predictable.

With pre-certified safety products, QNX Engineering Services and long-term support behind it, QNX becomes a long-term partner, not just a component within the device. It helps medical device manufacturers take a device from early concept through years of clinical service securely, reliably and safely.

November 2026

About QNX

QNX, a division of BlackBerry Limited, enhances the human experience and amplifies technology-driven industries, providing a trusted foundation for software-defined businesses to thrive. The business leads the way in delivering safe and secure operating systems, hypervisors, middleware, solutions, and development tools, along with support and services delivered by trusted embedded software experts. QNX® technology has been deployed in the world's most critical embedded systems, including more than 275 million vehicles on the road today. QNX® software is trusted across industries including automotive, medical devices, industrial controls, robotics, commercial vehicles, rail, and aerospace and defense. Founded in 1980, QNX is headquartered in Ottawa, Canada.

Learn more at qnx.com →

©2026 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY and EMBLEM Design, QNX and the QNX logo design are the trademarks or registered trademarks of BlackBerry Limited, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners. BlackBerry is not responsible for any third-party products or services.