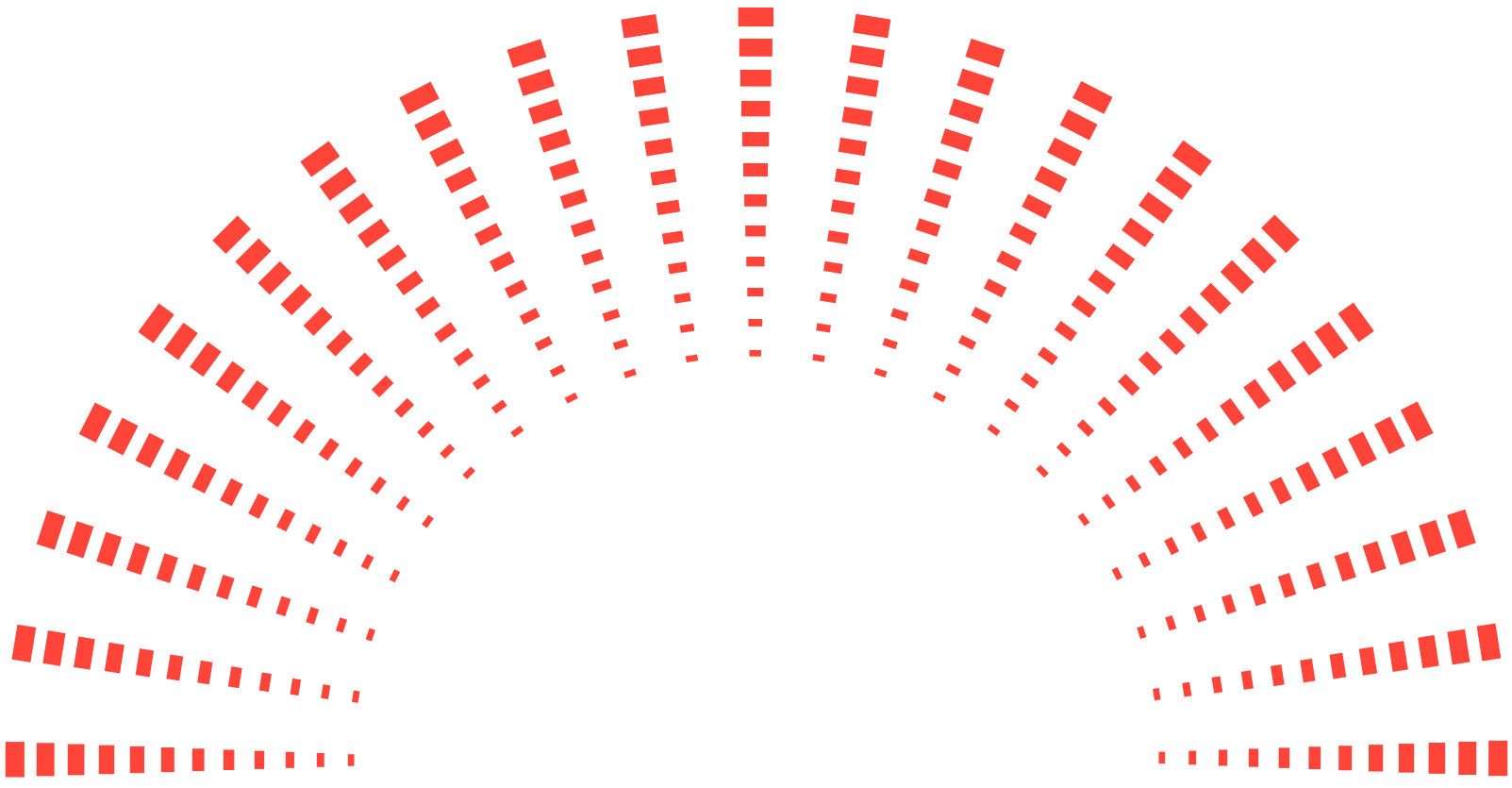
QNX

Solution Guide

Medical Devices

Foundational Software Solutions



Secure Software for Next-Gen Medical Devices

9/10 Medical Device Manufacturers Use QNX	**8/10** Surgical Robotics Manufacturers Use QNX	**100%** Success Rate in Achieving Safety Certification
Hundreds of Millions of Devices	**40+** Years Building Trusted Embedded Software	**50+** Types of Medical Devices Use QNX Solutions

Medical device manufacturers operate in an environment filled with intense market pressures, stringent safety regulations and concerns about cyberthreats. These manufacturers must also meet costly and difficult safety goals and create complex and connected software-defined designs. To ensure that medical devices are safe, reliable, secure and safety-certificable, manufacturers need to use a software foundation specifically designed for safety, cybersecurity and secure connectivity.

QNX® embedded software solutions help medical device manufacturers innovate and rapidly deliver safe, secure medical applications to market. Our solutions scale to meet the requirements of medical applications that range from small-footprint, real-time applications such as ventilators and infusion pumps to full-featured applications such as robotic surgery, imaging and monitoring systems. QNX provides a clear path from prototype to certified production-ready medical devices.

At QNX, we provide solutions that are trusted by leading medical device manufacturers. We also work closely with silicon partners such as the ARM® vendor ecosystem, Intel™ and major board vendors globally to deliver safe, secure and reliable software solutions.

Why Leading Medical Devices Companies Choose QNX

The same QNX software foundation that enables companies to build safety and cybersecurity into their products also simplifies safety certification, supports the reuse of legacy software, helps to improve reliability and enables innovation. QNX helps medical device manufacturers overcome many challenges at once.

We provide the confidence you need in building safety-critical software. QNX solutions are based on standards and offer proven software development tools classified to T3 and TCL3. The QNX® OS for Safety is pre-certified to IEC 62304 Class C. QNX® Hypervisor for Safety offers the same trusted functionality and performance as QNX® OS 8.0, plus virtualization support. QNX also offers solutions for safe communications, graphics, system libraries and middleware. And all our software is backed by decades of experience in providing trusted professional services.

At the heart of QNX is the microkernel QNX® OS 8.0. The microkernel architecture minimizes downtime and cyberattack surfaces through isolation and separation mechanisms. Device drivers and system services run alongside applications, separated from one another and the kernel. Running all OS services outside of kernel space enables highly available, fault-tolerant designs—the failure of one application or service will not crash the kernel, other services or other applications. Building on QNX software can help you to develop more resilient and reliable systems.

A microkernel RTOS also improves scalability and design flexibility. QNX RTOS scales from single-core to multicore to high-performance computing platforms seamlessly. For a system with limited capability and functionality, a microkernel can jettison excess services to fit in a small footprint with little memory. Developers can add drivers and services as needed. With virtualization support, the system can simultaneously run both new and legacy applications on multiple OSs.

Accelerate Safety Certification

Certifying a system to an industry safety standard such as IEC 62304 is time consuming and costly. The use of a safety-certified OS dramatically simplifies development and testing efforts and shortens overall system certification processes. The QNX OS for Safety is pre-certified to IEC 62304; and both the QNX OS for Safety and the QNX Hypervisor for Safety are certified for use in applications requiring IEC 61508 SIL 3. In addition, the QNX OS for Safety includes toolchains qualified to ISO 26262 and IEC 61508 TCL3 and T3 requirements. Safety-certified C and C++ libraries are also available.

Establish Reliability And Performance

Highly available, robust software systems for medical applications require a fail-proof foundation that enables them to boot quickly, run as specified and expected, avoid system crashes and ensure that the highest-priority tasks run first. The QNX OS 8.0's deterministic microkernel architecture provides such a foundation. Because drivers and services run outside the kernel space, the microkernel also enables the software components to be added and upgraded with minimal impact on the overall system.

Strengthen Cybersecurity

Connected medical devices are targets of cyberattacks, and the breach of a medical device or device communications can put patients, customers and your company at risk. Such devices may need to operate successfully on an IEC 80001-conformant healthcare IT network. Building and maintaining a secure system requires, at a minimum, a reliable and secure OS, a secure supply chain, and managed public key infrastructure (PKI) authentication. QNX solutions provide a layered approach to security that won't hamper functionality or performance.

• The QNX microkernel architecture has a much smaller attack surface compared to monolithic kernels, making it inherently more secure. Combined with a comprehensive suite of security features such as access control mechanisms—security policies, permission controls and DAC, encryption support, self-verifying filesystems and more—QNX provides a solid foundation for building secure end points.

Port Software Easily

When you design a prototype using Linux®, you can easily port your system into a production environment based on QNX. QNX products are POSIX compliant, so developers can easily port software from Linux or another OS to the QNX® Software Development Platform (SDP) with minimal redesign or recoding. In addition, developers ramp up quickly on QNX software because it looks and feels like Linux and uses familiar tools, such as the Eclipse-based QNX® Momentics® IDE, QNX Toolkit for Microsoft VS Code, and the GNU compiler collection (GCC).

With the QNX Hypervisor and the QNX Hypervisor for Safety, you can contain entire systems with their OSs as guests in hypervisor virtual machines. This, in turn, allows you to port legacy code onto new SoCs and run them concurrently with your latest product. You can also implement new features or upgrade entire systems in virtual machines, confident that the new code won't affect other systems—including safety-critical systems—running on the SoC.

• QNX provides a customer-centric cybersecurity solution to uncover and remediate software vulnerabilities in components from across your complex supply chain. This includes expert consulting services and customized software composition analysis and security testing tools

• BlackBerry® Certicom solutions make it easy to add cryptographic algorithms to medical devices, providing confidentiality, data integrity and authenticity without requiring cryptographic expertise. This solution includes managed PKI (Public Key Infrastructure) authentication and algorithms validated to FIPS (Federal Information Processing Standards), which is required to sell into U.S. Veterans Administration (VA) hospitals and other U.S. federal agencies.

Reduce Cost of Ownership

The reuse of application and driver code across devices and product lines helps you deliver new medical devices faster and drives more revenue with less risk of non-compliance. In contrast to the costly commitment of your resources to develop and maintain an open-source OS, such as Linux, QNX manages all OS maintenance and updates for you and frees your team to focus on innovative engineering of application software.

When you use QNX OS 8.0 and QNX software stack across product lines, you can offload OS maintenance to QNX, while sharing drivers and applications throughout your organization for a lower total cost of ownership. Plus, with POSIX compliance, switching from Linux or another OS to QNX is not a big lift. The result can be more efficient and more scalable engineering operations.

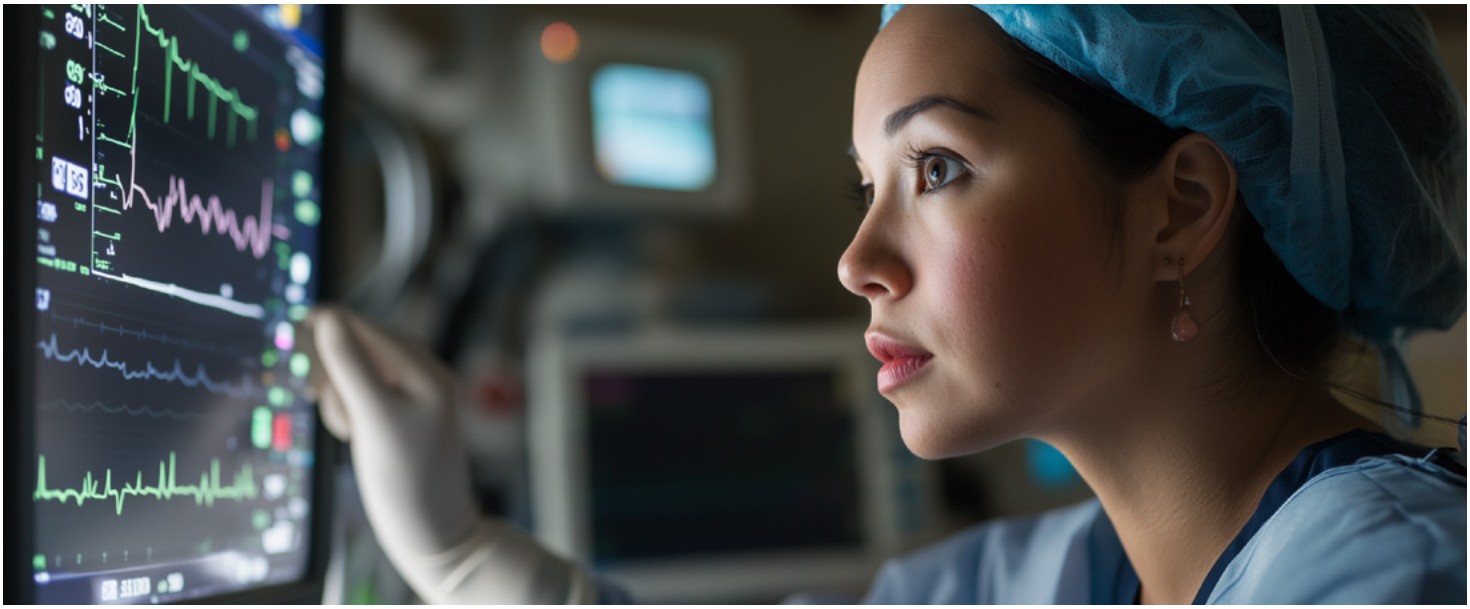
Silicon and Board Support

QNX® Board Support Packages (BSPs) provide an abstraction layer of hardware-specific software that facilitates the implementation of the QNX OS 8.0 on your board. Our extensive BSP library includes BSPs for SoCs manufactured by leading hardware manufacturers.

In addition, our professional services can develop customized solutions for you and support your safety and security requirements.

Learn more about our library of BSPs →

The QNX microkernel architecture isolates components that are not safety-critical from those that are, streamlining system certification processes.



Software Solutions for Medical Devices

Medical device companies globally trust QNX software for a broad range of life-critical and graphics-rich medical applications.

QNX provides time-tested and trusted foundation software, including the QNX OS 8.0, deterministic microkernel real-time operating systems; a safety-certified OS for Safety and Hypervisor for Safety, and cybersecurity services and tools—all of which are purpose-built for embedded systems. We also have experts who can provide the software, support and services you need to build better medical devices and get them certified and approved for market. We partner with you at every step, from the inception to the launch of your embedded system. We believe we are successful only when you are successful.

Solutions Built for Embedded System Security

Recent trends around consolidation of functions on a single system on a chip (SoC) and, increased connectivity and device complexity call for a new approach to security. For this reason, QNX delivers solutions that can help you secure your end products across the software development lifecycle and provide continued security measures once your products are in the field.

QNX's customer-centric cybersecurity solution is designed for complex and critical embedded systems like those within today's medical devices. With our expert consulting services and customized software composition analysis and security testing tools, we enable you to safeguard your products from cyberthreats by and uncover vulnerabilities that may exist within third-party software. We also examine your embedded software product for security vulnerabilities and software craftsmanship so you can continuously track and improve the quality of your software components.

BlackBerry® Certicom Asset Management System (AMS) helps medical device manufacturers to securely provision cryptographic keys, trust anchors and unique device identifiers and debug passwords, with visibility and governance over the manufacturing process. Its flexibility eliminates the need for ad hoc approaches to device provisioning and helps ensure a secure, traceable process throughout the supply chain.

Anesthesia	Medical Lasers
Angioplasty	Medical Ventilators
Artificial Hearts	Multi-Parameter Patient Monitors
Automated External Defibrillator	Multi-Spectral Imaging
Biological Warfare Detection	Neurological Monitors
Blood Analyzers	Nuclear Medicine
Blood Diagnostics	Nurse Call
Bone Densitometers	Nurse Monitoring
Cardiac Monitors	Organ Transportation Devices
C-Arm DR & Ultrasound	Pacemakers
Cataract Surgery	Patient Monitors
CPAP Machines	Peritoneal Dialysis
CTs and MRIs	PET & X-Rays
ECG and EKG	Plasma Collection
Electrical Stimulation	Point-of-Care (POC) Testing
Eye Lasers	Pulse Oximetry
Fluoroscopy	Rehab
Hemodialysis	Respiratory Care
Infusion pumps	Robotic Surgery Equipment
Laboratory Diagnostics	Sedation
LVAD (Left Ventricular Assist Device)	Sterilizers and Laboratory Equipment
Medical Exoskeleton Suits	Tissue Scanners
Medical Gateways	Vacuum Wound Management

QNX Support & Services

Proven Experience

Thousands of person-years in development, support and integration.

Service Excellence

100% success at meeting OEM start of production (SOP) deadlines.

Global Footprint

Regional experienced teams in US, EMEA and APAC.

Commitment

Dedicated, dependable and trusted staff.

Professional Services Expertise

Hardware

Prototyping, board support packages, driver development/customization, system optimization, fast boot, hypervisor support.

Porting & Integration

Linux/Android hypervisor guests, middleware integration, open-source porting/integration, legacy OS migration.

Safety & Security

Functional safety services, safety cases, hazard and risk analysis, penetration testing, security best practices, safety and security training.

Application

UI/UX design/development, application development, protocol development, middleware design and development, application stack design, application profiling and optimization.

Training

QNX offers hands-on, instructor-led training, online or in-person, using real-world examples to equip development teams with essential skills.

Consulting

Architectural reviews, on-site consulting (long/short term), cloud architecture integration, expert consultation, service retainers.

Learn more about our professional services and service packages →

Foundation Products/Initiatives

QNX Software Development Platform 8.0

QNX® Software Development Platform (SDP) 8.0 is the foundational development platform for the next generation of mission and safety-critical systems merging unprecedented performance with unparalleled security and reliability—without compromise. It features our next-generation QNX Operating System built on a future-ready architecture designed to maximize silicon advancements thanks to our advanced microkernel design.

Learn more →

https://blackberry.qnx.com/en/products/foundation-software/qnx-software-development-platform

QNX Advanced Virtualization Frameworks

Make use of our diverse set of industry-standard, hardware-independent frameworks to enable guest operating systems to share hardware and software services such as graphic displays, acoustic environments, touchscreens, media storage devices, video streams and cameras. The QNX® Advanced Virtualization Frameworks provide extended capabilities to the QNX Hypervisor.

Learn more →

https://blackberry.qnx.com/en/products/foundation-software/qnx-hypervisor/advanced-virtualization-frameworks

QNX Hypervisor

An embedded virtualization solution with a microkernel architecture so multiple OSs (Android, Linux, QNX) can safely operate on the same system-on-a-chip (SoC).

Learn more →

https://blackberry.qnx.com/en/products/foundation-software/qnx-hypervisor

QNX Accelerate

QNX® Accelerate is an initiative that makes cloud-enabled versions of our foundational products available. This reduces embedded software development cycles and improves time-to-market.

Learn more →

https://blackberry.qnx.com/en/products/accelerate

Safety-Certified Products

QNX OS for Safety

Built on the same microkernel architecture as the QNX® OS 8.0, the QNX OS for Safety is pre-certified to ISO 26262 ASIL D and to IEC 61508 SIL 3. Easily port Linux-based prototypes to the QNX Real-Time OS (RTOS) and get all the documentation and support you need for certification.

Learn more →

https://blackberry.qnx.com/en/products/safety-certified/qnx-os-for-safety

QNX Hypervisor for Safety

This real-time microkernel hypervisor provides the reliability and performance of the QNX OS and allows multiple OSs to safely operate in isolation and in parallel on the same system-on-a-chip (SoC). It is the first embedded hypervisor pre-certified to ISO 26262 ASIL D and to IEC 61508 SIL 3.

Learn more →

https://blackberry.qnx.com/en/products/safety-certified/qnx-hypervisor-for-safety

Security Solutions

QNX Cybersecurity

For more than 40 years, QNX has provided safe and secure embedded software solutions for automotive, industrial controls, robotics, medical devices, and other mission-critical applications. QNX cybersecurity is built on a strong culture, product excellence, and an ecosystem that enhances the company's security capabilities.

Learn more →

https://blackberry.qnx.com/en/products/security/qnx-security

Automotive Functions

QNX Cabin

QNX® Cabin is a hardware-portable, pre-integrated digital cockpit software reference implementation that provides a development framework for designing digital cockpit systems. By increasing software portability and supporting cloud-first development, QNX Cabin helps reduce development costs and accelerates time-to-market.

Learn more →

https://blackberry.qnx.com/en/products/automotive/qnx-cabin

QNX Multimedia Suite

The QNX® Multimedia Suite is middleware delivered with the QNX Software Development Platform. It can be implemented as an independent standalone system or fully integrated with other QNX products, including the QNX Platform for ADAS.

Learn more →

https://blackberry.qnx.com/en/products/automotive/multimedia

QNX Platform for ADAS

QNX® Platform for ADAS is a foundation for building ADAS and automated driving applications. The modular, sensor/processor-agnostic framework allows for code to be written once and re-used. Optimized for automotive silicon and compatible with a variety of processing cores.

Learn more →

https://blackberry.qnx.com/en/products/automotive/qnx-adas

QNX Sound

QNX® Sound is a holistic software environment that lets you design the next generation of vehicle audio with a holistic software environment that manages the entire vehicle soundscape.

Learn more →

https://blackberry.qnx.com/en/products/automotive/qnx-sound

May 2025

QNX

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 255 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 →