

QNX OS for Security

Common Criteria certified, memory-protected, microkernel architecture for maximum reliability, unparalleled scalability, and realtime performance.

Since 1980, manufacturers have relied on QNX® realtime OS technology to power mission-critical applications – everything from medical instruments and 9-1-1 call centers, through battlefield communications and nuclear-monitoring systems, to Internet routers and in-car infotainment devices. Small or large, simple or distributed, these systems share an unmatched reputation for security and reliability, operating 24 hours a day, 365 days a year.

Leverage multi-core processing

Not only is the QNX OS for Security the only full-featured realtime OS to achieve Common Criteria certification, it is the only Common Criteria certified realtime OS to implement symmetric multiprocessing (SMP) and bound multiprocessing (BMP) for multi-core processors. As a result, it is the only certified realtime OS to support the parallelism necessary for successful multi-core designs.

Build secure systems

QNX adaptive partitioning technology guarantees system resources for applications while preventing rogue software from denying resources to other parts of a system. During overload conditions, adaptive partitioning enforces hard resource guarantees, ensuring applications receive their budgeted share of resources.

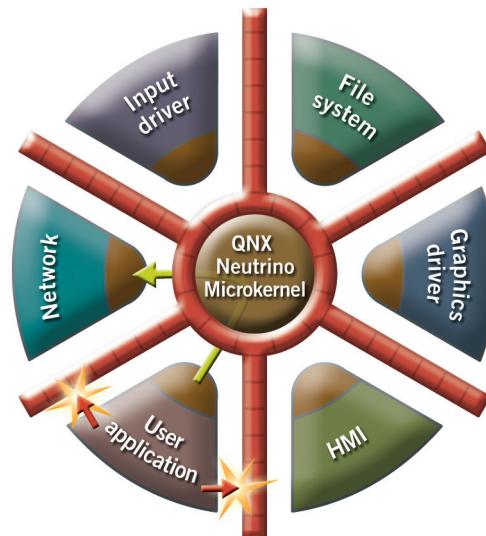
Create fault tolerant applications

Time-tested and field-proven, the QNX Neutrino® RTOS that the QNX OS for Security is based on, is built on a true microkernel architecture. Under this system, every driver, application, protocol stack, and file system runs outside the kernel in the safety of memory-protected user space. Virtually any component can fail and be automatically restarted without affecting other components or the kernel. Further, the QNX OS provides an optional high-availability framework for ensuring critical software is monitored and kept running even after faults. No other commercial RTOS provides such a high level of fault containment and recovery.

Inherently modular, the QNX OS lets you dynamically upgrade modules, introduce new features, or deploy bug fixes – without costly downtime or system outages.

Rely on standards for secure programming

Engineered to the POSIX PSE52 Realtime Controller 1003.13-2003 standard, the QNX OS provides a well understood programming API with predictable and reliable behavior – a key ingredient to secure systems. This POSIX API makes it unnecessary to use proprietary interfaces that have the potential for insecure behavior and misunderstood results.



Secure microkernel by design – A microkernel realtime operating system provides protective barriers between processes including networking and filesystems, which are typically within the kernel memory space in monolithic operating systems.

Moreover, POSIX demands proper adherence to user and group privileges and security defaults that prevent, if necessary, high privilege access to system resources. Using POSIX programming also gives developers the power to port legacy and open source UNIX, Linux, and Internet code with just a simple recompile. With standard APIs, developers can reuse application code, avoid costly delays, and shorten their learning curve – accelerating development cycles and reducing time to market.

Scale large or small

Take advantage of the inherent multi-core capability and built-in transparent distributed processing of the QNX OS to create large,

highly fault-tolerant systems. Regardless of design requirements, developers can use the same OS, tools, APIs, and source code for all projects. The result? Longer product life cycles, shorter development time, and a significant return on investment.

Foundry27

This community portal for QNX developers provides software updates, board support packages, drivers, forums, and wikis. Whether developers want to discuss ideas, post questions or answers about developing with QNX, or download drivers for the latest hardware, Foundry27 offers the resources required.

QNX OS for Security at a glance

Common Criteria ISO/IEC 15408 EAL 4+ certification

- Stringent standard for security and development processes used in development
- First full-featured EAL 4+-certified realtime operating system
- First realtime operating system to include SMP support for multi-core processors and adaptive partitioning technology in certification

Microkernel architecture

- Dynamically upgradable services and applications
- Fine-grained fault isolation and recovery
- Message-passing for modular, well formed systems

POSIX compliance

- POSIX PSE 52 support of broadest range of POSIX API specifications
- Well understood programming API with predictable behavior
- Correct user and group privilege management and enforcement

High availability and fault tolerance

- Heartbeat for early fault detection
- Intelligent restart and transparent reconnection

Adaptive partitioning

- Guaranteed system resources for secure, reliable systems without compromised performance and flexibility

Predictable realtime performance

- Preemptive scheduler with choice of scheduling methods
- Distributed priority inheritance

Multi-core

- Comprehensive multi-core support
- Asymmetric, symmetric, and bound multiprocessing
- Simple migration from uniprocessing to multiprocessing

Transparent distributed processing

- Transparent network access to remote resources
- Simplified design of fault-tolerant clusters

Filesystems

- Image, RAM, Flash, QNX, Linux, DOS, CD-ROM, DVD, NFS, CIFS, Compression, NTFS, and HFS+
- Power safe mass storage file system

Resource manager framework

- Device drivers implemented in user or nonkernel space
- Ability to start, stop, and debug drivers like any standard application

Device drivers

- Audio, character, disk, graphics, input, networking, parallel, printer, serial, and USB

Processor support

- ARM, PowerPC, and x86

About QNX Software Systems

QNX Software Systems Limited, a subsidiary of BlackBerry, is a leading vendor of operating systems, development tools, and professional services for connected embedded systems. Global leaders such as Audi, Cisco, General Electric, Lockheed Martin, and Siemens depend on QNX technology for vehicle infotainment units, network routers, medical devices, industrial automation systems, security and defense systems, and other mission- or life-critical applications. Founded in 1980, QNX Software Systems Limited is headquartered in Ottawa, Canada; its products are distributed in more than 100 countries worldwide. [Visit www.qnx.com](http://www.qnx.com)