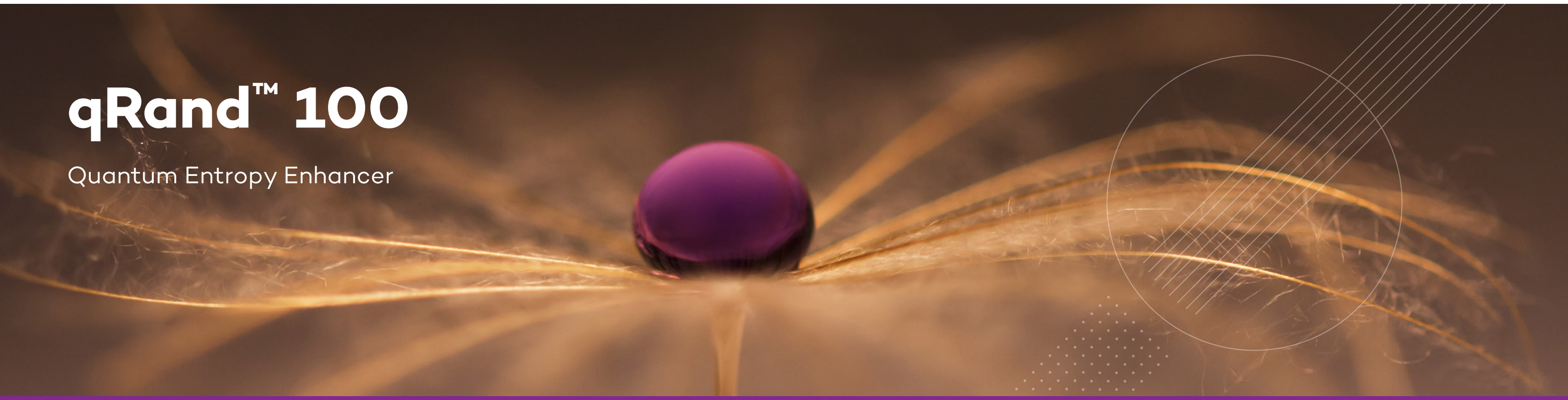
Quintessence Labs



qRand™ 100

Quantum Entropy Enhancer

Feeds quantum random numbers to the entropy pool of a computer

Prevents issues when /dev/random blocks due to insufficient entropy

Ensures applications always have sufficient entropy, even in virtual environments

Overview

QuintessenceLabs' qRand 100 entropy enhancer augments a computer's entropy pool with full entropy random bits, solving the problem of "entropy starvation". This prevents performance degradation for applications that use entropy, or the security compromise of using low entropy pseudo-randomness.

The Challenge of Entropy Limitations

The qRand 100 entropy enhancer solves the problem of "entropy starvation", by augmenting a computer's entropy pool when it falls below a lower bound.

Entropy starvation is a major concern, especially in environments using virtual machines, including in cloud infrastructure. It degrades performance, with applications failing to respond due to a lack of randomness for cryptographic operations. Equally worrisome is the fact that many applications use a "non-blocking" source of pseudo randomness to overcome this first issue. This can compromise security, resulting in vulnerabilities, including duplicate cryptographic keys.

RNG in Linux

Any process that needs random numbers can get them from /dev/random. However, /dev/random will only return random numbers if there is enough entropy available. If not, /dev/random simply blocks, resulting in performance degradation. Many applications remedy this using "non-blocking" sources of randomness such as /dev/urandom. This degrades security, resulting in potential vulnerabilities such as duplicated cryptographic keys. Other Linux packages that provide random numbers like "rngd" and "haveged" can also result in entropy dilution if insufficient entropy is available, with the potential for security risks.

This is particularly challenging in environments where normal entropy gathering does not yield enough entropy, for example in virtual machines or embedded devices.

The qRand 100 entropy enhancer addresses these issues by feeding entropy into the entropy-pool of a computer. The entropy provided is delivered from QuintessenceLabs' qStream™ 200 quantum random number generator (QRNG) appliance.

How qRand 100 Works

The qRand 100 entropy enhancer monitors entropy status on a computer, and when it falls below a defined lower bound, augments it with entropy from QuintessenceLabs' quantum random number generator (QRNG), embedded in the Trusted Security Foundation® (TSF®) key and policy manager appliance. This enables applications on the computer to generate and use high quality cryptographic keys without any changes to the application itself.

Users can configure the behavior of the qRand 100 entropy enhancer in several ways, such as setting the lower limit of the entropy status, the order of TSF key and policy manager devices from which to get entropy, and logging options.

QuintessenceLabs' QRNG

QuintessenceLabs' uses groundbreaking quantum technology to deliver random numbers with full-entropy at 1 Gbit/sec. The QRNG is available as the qStream™ 200 stand-alone appliance or qStream 100 PCIe card, or as part of the TSF key and policy manager product suite.

SPECIFICATIONS

qRand™ 100

Quantum-powered entropy

Key Features

- Linux daemon, running as a native system service, that monitors entropy status in system
- When entropy levels fall below lower limit, qRand 100 retrieves entropy from the quantum random number generator (QRNG) embedded in TSF 300 or TSF 400
- User configurable

User settings

- Lower bound of entropy (in bits)
- Entropy fill watermark (in bits)
- Enable/disable use of deterministic entropy sources
- Select from any available TSF random objects
- Enable/disable audit logging; log verbosity level

Supported OS

- Ubuntu (64-bit) 16.04, 18.04
- RHEL (64-bit) 6.10, 7.3, 7.6
- Support for more Linux distributions planned

TSF 300 or TSF 400

Refer to the TSF product sheet for full specifications. Includes quantum random number generator with the following features:

- Quantum random number generator delivering 100% entropy
- 8 Gbit/sec quantum entropy source, 1Gbit/sec conditioned entropy
- Meets all requirements of NIST SP 800-90A, 90B and 90C (draft) standards for Non-Deterministic Random Bit Generators
- Satisfies NIST SP 800-22 (NIST STS) and Dieharder tests