Quintessence Labs

qStream™ Plus

Quantum Entropy Appliance

Generates and supplies highest quality entropy throughout your network

Combines quantum random number appliance with entropy management software

Ensures your organization always has sufficient entropy

Overview

When it comes to data security, the quality and quantity of random numbers have a big impact. Weak random numbers generated through algorithmic means, as well as insufficient quantity of high-quality random numbers, increase the risk of a breach and data loss. This is particularly challenging for virtual machines and embedded devices where normal operation may not yield enough entropy.

QuintessenceLabs' qStream Plus Quantum Entropy Appliance combines our high-speed quantum random number generator appliance qStream with the qRand entropy enhancer. It delivers the highest quality random numbers at high speeds, and uses them to seamlessly augment the entropy pool of computers and networks. This prevents performance degradation for applications using entropy, and the security compromise of using low-entropy pseudo-random numbers.

Quantum Random Number Generator

The qStream Plus Quantum Entropy Appliance uses quantum tunneling to deliver random numbers with full entropy at 1 Gbit/s. This delivers both the randomness and the speed needed by organizations of all sizes for secure operations.

Augmenting Entropy

Organizations using random numbers to secure their data can get them from /dev/random. However, this function only returns random numbers if there is enough entropy available. If not, it simply blocks, degrading performance. An alternative is to use "non-blocking" sources of random number such as /dev/urandom. However, this approach degrades security, potentially resulting in vulnerabilities such as duplicated cryptographic keys.

The qRand entropy enhancer monitors the entropy status on a computer, and augments it with entropy when it falls below a defined lower bound. This enables applications on the computer to generate and use high quality cryptographic keys without any changes to the application itself.

Service Use Case

The IT infrastructure of a major financial institution is deployed in multiple data centers in the USA, Europe and Asia. Most applications are hosted on virtual servers.

QuintessenceLabs entropy appliances were configured as high availability clusters across data centers in each geographic region. qRand was deployed in the guest VMs to ensure that the entropy pool of each virtual server always has sufficient random to satisfy the needs of all applications running on these servers.

qRand instances connect to one or more appliance clusters to retrieve quantum entropy when required. Automatic failover within and across clusters ensures that no server is ever depleted of high quality random.

SPECIFICATIONS

qStream™ 100A

Appliance quantum random number generator

Configuration	**Rackmount Appliance** • Dimensions: 1RU: H: 4.28 cm (1.69"), W: 48.20 cm (18.98"), D: 80.85 cm (31.83") • Power Supply: 1RU: Dual, redundant, hot-swappable, 550W • Support for running multiple Virtual Machines (VMs)
Performance	• 8 Gbit/s quantum entropy source • Outputs: up to 1 Gbit/sec conditioned entropy (QRNG) up to 1 Gbit/sec unconditioned entropy
Operations	• Raw and conditioned entropy output (via TCP and TLS) • Hardened OS • Granular, auditable access control • Attended or unattended startup • Logging of events and audits
Standards & Interoperability	• 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 • Supports PKCS#11 over KMIP • OASIS KMIP: Conformant with standards 1.0/1.1/1.2/1.3/1.4/2.0 plus extensions for secure Random Object management
Administration & Management	• Web (HTTPS) or command-line (SSH) management interfaces • Purpose-built QRE secure operating system • Delivered with qClient SDK

qRand™

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 retrieves entropy from the quantum random number generator embedded in qStream 100A, qCrypt 300R or 350TSF • 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 qCrypt 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
Supported Entropy Sources	Refer to adjacent qStream 100A specifications or qCrypt product sheet for full specifications. Includes quantum random number generator with the following features: • Quantum random number generator delivering full 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

Quintessence Labs

AUSTRALIA
Unit 1, Lower Ground
15 Denison St
Deakin, ACT 2600
+61 2 6260 4922

UNITED STATES
175 Bernal Road
Suite 220
San Jose CA 95119
+1 650 870 9920

www.quintessencelabs.com

Document ID: 4490