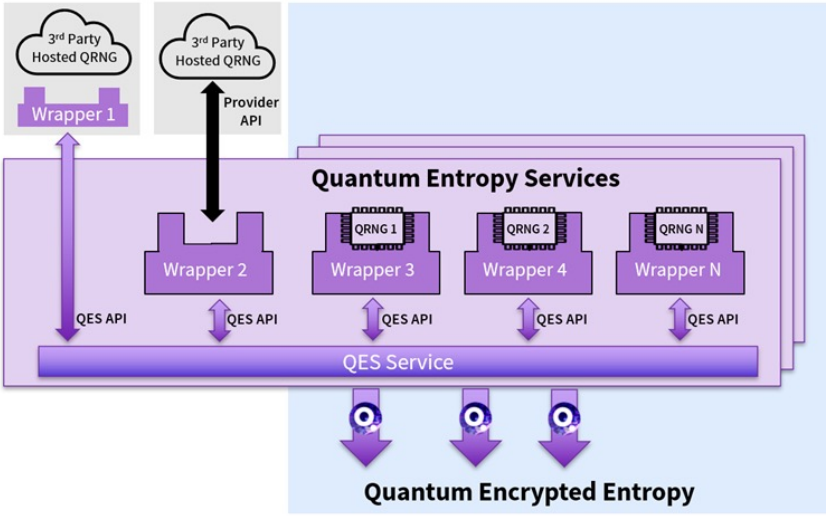
quantropi
Bring it on.

QiSpace™ Quantum Entropy as a Service (QEaaS)

QiSpace™ QEaaS is a scalable and resilient hybrid SaaS solution providing a secure distribution network for strong entropy to any endpoint over existing IP networks. QEaaS immediately hardens cryptographic security by enabling existing algorithms to achieve their full security potential via true random keys. QiSpace™ sources its quantum entropy from various industry leading QRNG vendors and provides generation and quantum-secure distribution performance up to 1Gbps over existing network infrastructure.



Key Highlights

- QRNG outputs are extracted through a standardized services layer. Quantropi hosted QRNG hardware is provisioned across multiple worldwide data center locations or via external 3rd Party Hosted QRNG Services.
- Customer hosted QRNG option to support air gapped implementations or strict security requirements.
- 3rd Party Entropy acquired via classically secure Provider APIs is conditioned / privatized via QE2QK mechanism to protect from injection attacks.
- QiSpace™ entropy distribution is protected using Quantropi' Quantum Permutation Pad technology and is "double wrapped" with AES-256 TLS encryption to preserve FIPS compliance.
- **SEQUR Nject** component adds quantum generated strong random into the OS entropy pool to prevent entropy starvation and transparently harden all applications and functions that rely on OS entropy.
- **SEQUR NGen** is a pseudorandom number generator for offline usage that provides significantly greater entropy (up to 100K bits) than classical PRNGs, yielding output bits with periodicity approaching infinity.

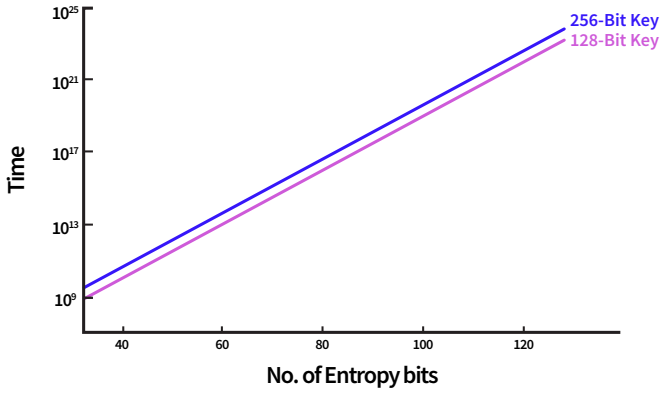
V02/2023.05.30

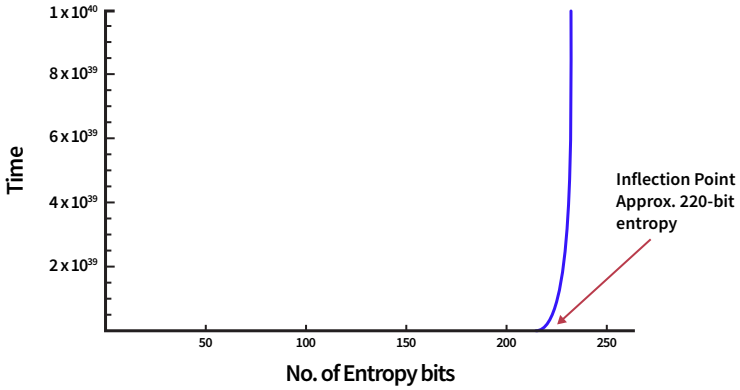
quantropi
Bring it on.

Why Does Entropy Matter?

Entropy, or randomness, is the foundation for operating system security: cryptographic keys, TLS nonces, ASLR offsets, password salts, TCP sequence numbers, and DNS source port numbers all rely on a source of hard-to-predict random bits. Using sources of strong entropy increases the hardness for all of these elements.

Accelerating innovation in new technologies including AI/ML and quantum computing have ushered in a new era of more robust and sophisticated attacks on low entropy systems. In fact, a 2023 ATIS report found that increasing AES key lengths alone from 128 to 256-bits did not significantly increase protection from a quantum brute force attack. In ordered to achieve significant protection against Grover's algorithm an increase in entropy is required, specifically the 256-bit key required at least 220 bits of strong entropy. Quantum Random Number Generators "QRNGs" are sources of strong entropy, however it's not feasible to co-locate a physical QRNG hardware source with every endpoint requiring entropy.

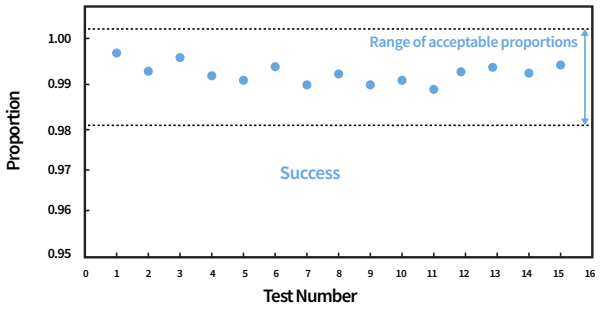




Entropy Quality

QiSpace™ generated entropy quality is validated using a robust set of industry standard statistical testing tools with audit reporting available. The results pictured below were obtained from a QiSpace entropy sample.

A. NIST Statistical Test Suite Results



B. ENT Test Results

ENT Test Summary	Ideal Value	Test Value
Entropy per 8 bits	8.0 bits	8.000000 bits
Optimum compression	0%	0%
Chi Square Distribution p-value	253 1%-99%	248.04 61.08%
Arithmetic Mean	127.5	127.4987
Monte Carlo Pi	3.141592645	3.141660422
Serial Correlation	0	0.000011

C. DIEHARDER Test Results

DIEHARDER	Results
Passes	113
Weak	1
Failed	0

For Pricing and Availability Contact:

Quantropi Inc.
1545 Carling Ave, Suite 620
Ottawa ON, K1Z 8P9 CANDA
+1 (613) 695-5711
www.quantropi.com