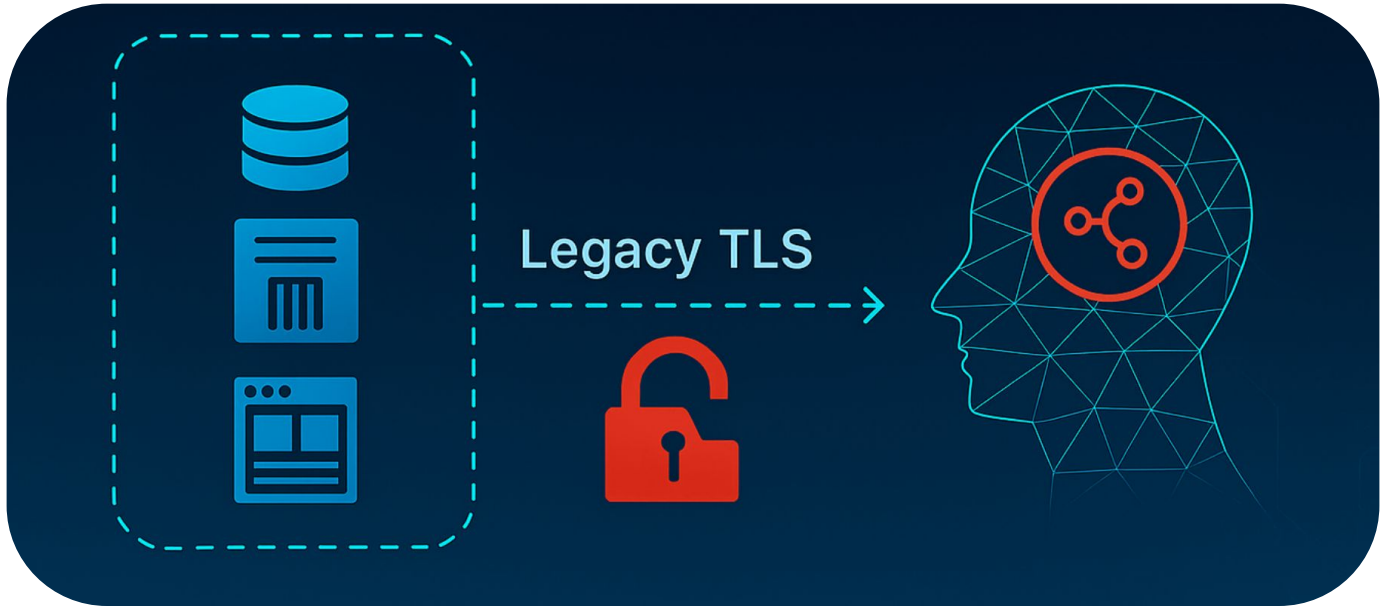
quantropi®
Bring it on.

Proxy-Q

Proposed Configuration for COVENCO

PQC Challenges for Legacy IBM systems

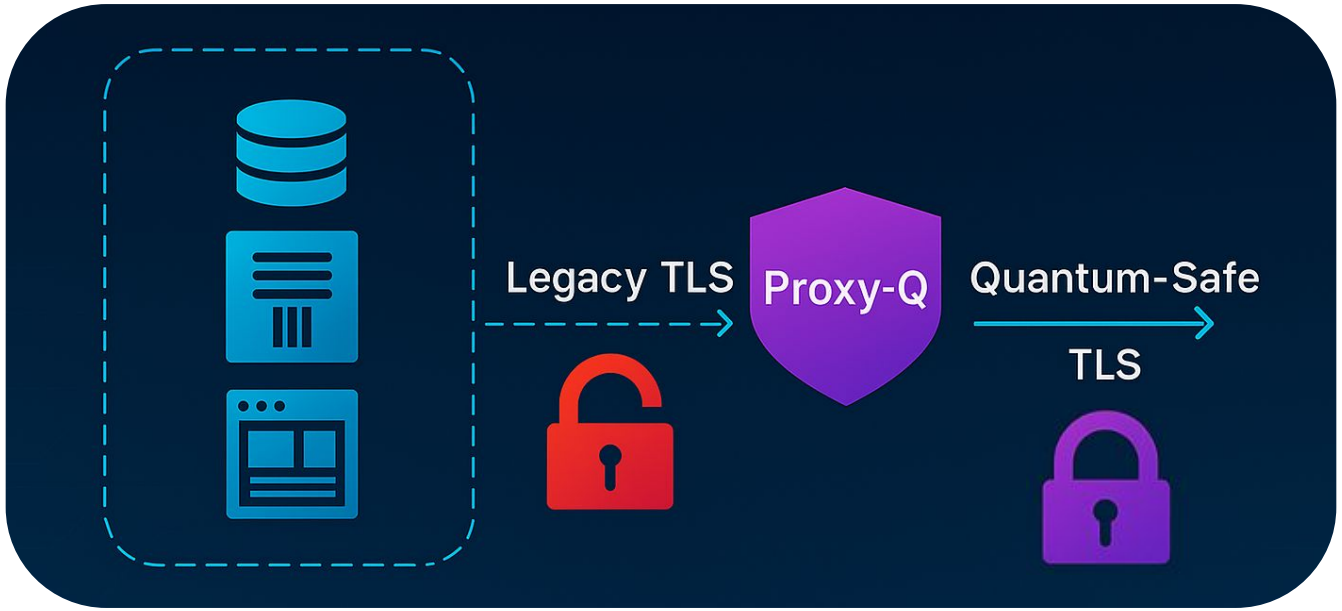
A growing number of enterprises still rely on IBM systems that **cannot be upgraded** to post-quantum cryptography, leaving **critical data flows exposed** to Harvest-Now & Decrypt-Later risk and **inconsistent legacy TLS** configurations.



quantropi

Introducing “Proxy-Q”

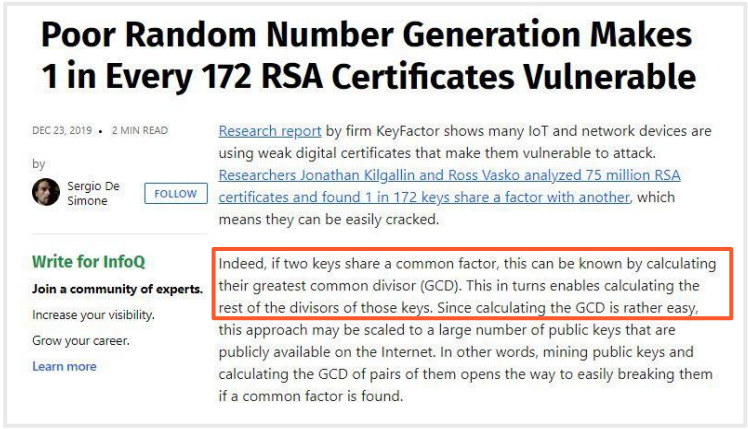
Routing all IBM traffic through **“Proxy-Q”** creates a **quantum-safe perimeter** around these unchangeable systems, delivering **modern security and centralized control** without touching any of the underlying IBM workloads.



quantropi

Powering Proxy-Q with Strong Entropy

Weak Entropy = Weak Keys. Proxy-Q creates **strong keys** using entropy from **Quantum Random Number Generators** (QRNGs), streamed securely over the network by **QiSpace Enterprise Servers**.



Poor Random Number Generation Makes 1 in Every 172 RSA Certificates Vulnerable

DEC 23, 2019 • 2 MIN READ

by

Sergio De Simone FOLLOW

Write for InfoQ

Join a community of experts.

Increase your visibility.

Grow your career.

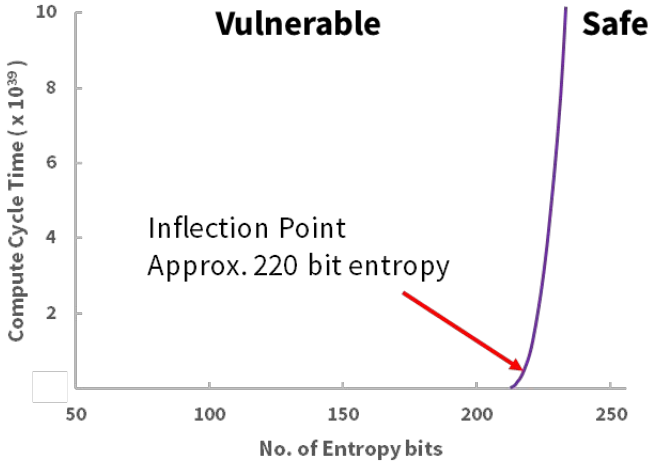
Learn more

Research report by firm KeyFactor shows many IoT and network devices are using weak digital certificates that make them vulnerable to attack. Researchers Jonathan Kilgallin and Ross Vasko analyzed 75 million RSA certificates and found 1 in 172 keys share a factor with another, which means they can be easily cracked.

Indeed, if two keys share a common factor, this can be known by calculating their greatest common divisor (GCD). This in turns enables calculating the rest of the divisors of those keys. Since calculating the GCD is rather easy, this approach may be scaled to a large number of public keys that are publicly available on the Internet. In other words, mining public keys and calculating the GCD of pairs of them opens the way to easily breaking them if a common factor is found.

2019 Key Factor Study: RSA certificates generated with low quality random were more susceptible to compromise.

Poor Random Number Generation Makes 1 in Every 172 RSA Certificates Vulnerable Keyfactor Research Report: Factoring RSA Keys in the IoT Era (2019)



Run Time of Grover's Algorithm to Break AES 256-bit Encryption Using a 256-bit Key Across Entropy Range

Entropy Rate = 220/256 = 0.85 minimum!

ATIS, 2023. Implications of Entropy on Symmetric Key Encryption Resilience to Quantum

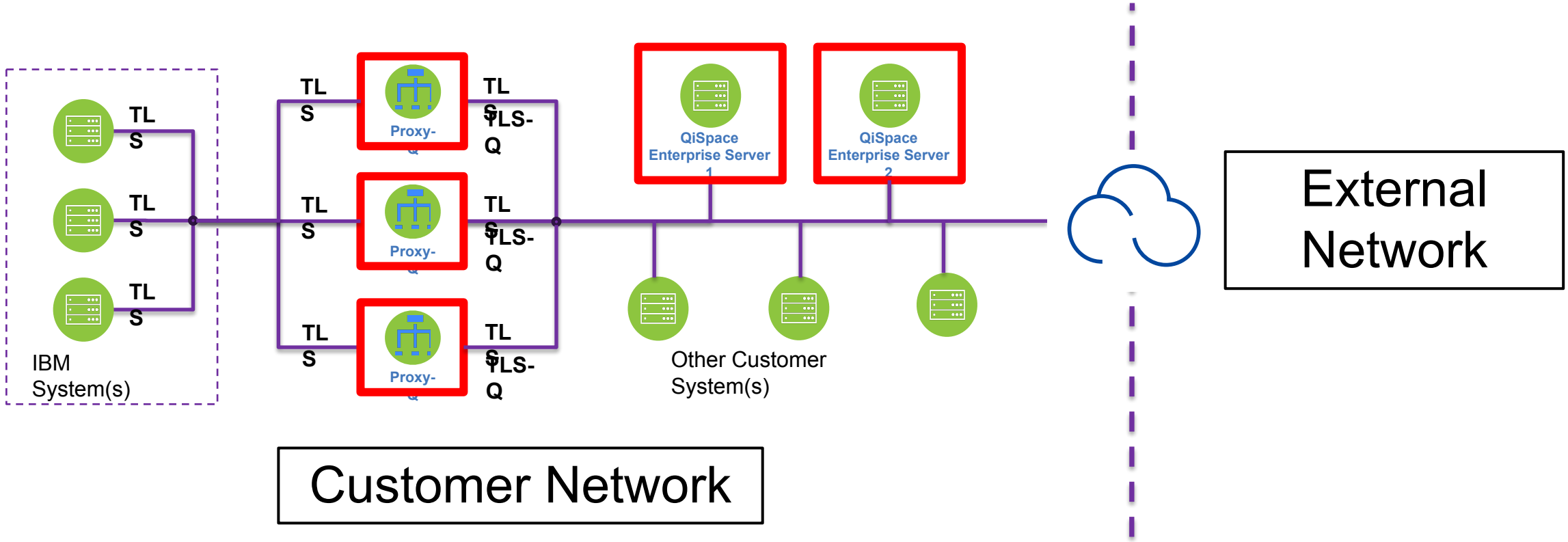
quantropi

Quantropi's QRNG Differentiators

- **Entropy Sovereignty:** Customers have complete ownership and control over where their entropy is generated and how it is stored and used.
- **Multisource QRNG Generation:** QiSpace™ hosts a multisource portfolio of industry leading quantum random number generators to ensure entropy source diversity.
- **Quantum Secure Distribution:** QiSpace™ uses quantum secure symmetric encryption for transmissions to enable high-performance distribution, at gigabits per second, over existing internet infrastructure.
- **Entropy Expansion:** QiSpace™ provides platform resiliency against peak demand and flexibility for connection limited and offline endpoints.

quantropi

Proxy-Q Implementation for IBM Systems



Routing all IBM legacy traffic through Proxy-Q layer delivers operational, security, compliance, and lifecycle advantages.

quantropi

Security Advantages

- Instant PQC protection for all IBM systems without touching them — legacy TLS stacks (GSKit, System SSL, Java 6/7 runtimes, MQ channels, DB2 clients, CICS/IMS connectors) remain unchanged while Proxy-Q upgrades the crypto on the wire.
- Eliminates Harvest-Now, Decrypt-Later exposure — even if IBM endpoints negotiate RSA/ECC, the Proxy-Q → destination leg is PQC-hardened.
- Creates a uniform quantum-safe perimeter — instead of dozens of inconsistent cipher configurations across LPARs, partitions, and middleware.
- Prevents downgrade attacks — Proxy-Q enforces PQC outbound even if inbound traffic is classical.
- Centralizes certificate and key lifecycle — no need to manage certs inside AIX keystores, RACF, GSKit, or Java trust stores.
- Allows hybrid PQC adoption — Proxy-Q can run hybrid (PQC + classical) even if IBM stacks cannot.
- Isolates weak IBM crypto implementations — protects systems still using TLS 1.0/1.1, SHA-1, or outdated cipher suites.

Architectural & Operational Advantages

- Zero-touch for IBM systems — no changes to OS, middleware, configuration files, or application code.
- Stability preserved — avoids the risk of modifying mission-critical workloads (COBOL, RPG, MQ, DB2, WebSphere ND, TPF).
- Central enforcement point — one place to enforce PQC, TLS policies, cipher suites, and routing logic.
- Consistent behavior across heterogeneous IBM environments — AIX, i/Series, z/OS, Linux on Power all benefit equally.
- Supports phased migration — customer can modernize endpoints gradually while PQC is already deployed.
- Reduces dependency on IBM's PQC roadmap
- Simplifies troubleshooting — Proxy-Q provides visibility into encrypted flows that IBM systems normally hide.
- Allows traffic shaping, load balancing, and HA — capabilities IBM stacks often lack natively.
- Decouples crypto from application lifecycle — crypto agility becomes an infrastructure function, not an app function.

Integration & Compatibility Advantages

- Works with any IBM protocol that rides TLS — MQ, DB2, WebSphere, REST APIs, SOAP, LDAP, custom TCP.
- Supports legacy clients that cannot be upgraded — old Java runtimes, old MQ clients, old GSKit versions.
- Bridges incompatible cipher suites — Proxy-Q can accept weak inbound ciphers and enforce strong PQC outbound.
- Provides a uniform interface to non-IBM systems — cloud, microservices, modern apps, SaaS endpoints.
- Allows PQC tunneling for non-TLS IBM protocols — when wrapped or proxied appropriately.

Compliance & Governance Advantages

- Accelerates PQC compliance — meets NIST, NSA CNSA 2.0, and industry PQC mandates without waiting for IBM.
- In UK - meets the Cyber Assessment Framework principles
- In Europe - meets the Cyber Resilience Act
- Reduces audit scope — auditors focus on Proxy-Q rather than dozens of IBM systems.
- Provides centralized logging and attestation — cryptographic posture becomes known, measurable and reportable.
- Supports regulatory requirements for crypto agility — which IBM legacy stacks cannot meet on their own.

Cost, Risk & Lifecycle Advantages

- Avoids expensive IBM upgrades — many PQC-related upgrades require OS migrations, new hardware, or unsupported patches.
- Extends the life of stable IBM workloads — customer keeps “don’t-touch” systems running safely for years.
- Reduces operational risk — no need to modify brittle COBOL/RPG apps or ancient middleware.
- Avoids vendor lock-in — PQC strategy becomes independent of IBM’s slow release cycles.
- Provides a predictable, centralized upgrade path — when PQC standards evolve, only Proxy-Q needs updating.

Network & Performance Advantages

- Offloads heavy crypto from IBM systems — many Power and z/OS workloads are CPU-sensitive; PQC offload avoids performance hits.
- Enables connection pooling and reuse — reducing overhead on IBM backends.
- Allows intelligent routing — PQC-protected traffic can be steered to modern services, clouds, or external partners.
- Supports HA and failover — Proxy-Q can be clustered, something many IBM stacks cannot do for TLS termination.

Bill Of Materials & Budgetary Pricing

QiSpace Enterprise Server	
VM/Hardware	
	4 CPU (x86, 64bit)
	8 GB RAM
	100 GB SSD
	1 x 1 GbE NIC
Software	
	RHEL
	QiSpace Enterprise Server

QiSpace Proxy-Q Server	
VM/Hardware	
	4 CPU (x86, 64bit)
	16 GB RAM
	32 GB SSD
	1 x 1 GbE NIC
Software	
	RHEL
	QiSpace Proxy-Q Server

* Bill of Materials only includes hardware and software components. It does not include networking equipment.

QiSpace Proxy-Q Annual Subscription Pricing		
License	**Description**	**Base Price**
Standard	Single instance, Non-production, testing, DR	$25,000
Enterprise	Single instance, Production	$60,000
High Availability Options		
HA Pair (2)	Two Load-balanced or failover pair for one logical segment	1.5x Base Price
HA Triple (3)	Three Load-balanced or failover triple for one logical segment	2.0x Base Price
Fleet	4+ instances across multiple segments or sites	Volume Discount

* QiSpace Enterprise licensing included with purchase of Proxy-Q

quantropi

quantropi
Bring it on.

Richard Brooks
Blue Mesh Solutions
richard@bluemeshsolutions.com

Jay Toth
Quantropi
jay.toth@quantropi.com

Bring it On.