covenco
DATA MANAGEMENT & INFRASTRUCTURE 365

GUIDE

Is your encryption ready for the Quantum Age?

A practical guide for IT leaders on protecting encrypted data in a post-quantum world.

quantropi®
Bring it on.

Who this relates to:

Organisations running encryption-dependent infrastructure where long-term data sensitivity creates exposure to future quantum decryption. Particularly relevant to those using IPSec, VPN, TLS, or MACsec across financial services, healthcare, legal, public sector, manufacturing, and critical national infrastructure.

What this guide covers:

- Why current encryption is vulnerable to a new class of attack
- What Harvest Now, Decrypt Later means for your organisation
- How IBM Power and legacy systems create specific exposure
- How Digital QKD eliminates the key distribution risk
- How the quantum-safe forward proxy protects systems you cannot re-engineer
- A practical route to post-quantum readiness with Covenco and Quantropi

Solutions discussed:

- Quantum encryption risk assessment
- Digital Quantum Key Distribution (D-QKD)
- Quantum-safe forward proxy for legacy systems
- Post-quantum cryptographic standards alignmen
- On-premise, hybrid, and cloud deployment options

The only TrUE Quantum-Secure Cryptography Platform

The problem is not your firewall. It is your key exchange.

Most organisations assume their encryption is doing its job. Firewalls are in place. VPNs are active. TLS is running across every connection. The security stack looks sound.

But a new class of attack does not need to break your encryption today. It only needs to capture your data and wait.

The protocols most enterprises rely on, IPSec, VPN, TLS, and MACsec, were designed for a world without quantum computing. The encryption algorithms are sound against today's computers. Against a sufficiently capable quantum machine, RSA and ECC, the foundations of most enterprise key exchange, can be broken systematically.

This is not a distant risk. It is a structural vulnerability in the cryptographic foundations that all current security relies on.

NIST published its first post-quantum cryptographic standards in 2024, FIPS 203, 204, and 205, confirming that migration is no longer speculative. It is a structured, time-bound requirement for regulated organisations and government suppliers. The UK's National Cyber Security Centre has issued migration guidance for regulated organisations.

The question for most IT Directors and security leads is no longer whether to act. It is when, and where to start. This guide explains the threat, the standards, the specific challenge of legacy systems, and the two practical deployment paths that Covenco and Quantropi offer to address it.

> ***"The encryption protecting your data today was not designed for the computers being built right now."***

Comparison: classical encryption vs quantum-safe encryption

Metric	Classical Encryption	Quantum-Safe (QiSpace)
Key exchange	Keys transmitted over the data path	Keys derived at each endpoint, never transmitted
HNDL vulnerability	High. Captured traffic includes keys.	Eliminated. No keys exist in transit.
Legacy system support	Requires modification or replacement	Proxy architecture. No device modification needed.
Hardware requirement	Standard IP infrastructure	Software-defined. No quantum hardware required.
NIST alignment	RSA and ECC not post-quantum safe	Aligned to FIPS 203, 204, and 205.

THE HNDL THREAT

Harvest Now, Decrypt Later: what it is, who is at risk, and why the timeline matters now.

The attack does not require quantum capability to begin. It requires only that adversaries capture and store encrypted traffic today, which they are already doing.

Nation-state actors and sophisticated criminal organisations are intercepting encrypted data across financial services, healthcare, legal, and government networks. Not to read it now. To hold it until quantum computing matures, at which point decryption becomes straightforward. This is Harvest Now, Decrypt Later, HNDL, and it is active now.

Y2Q, the point at which quantum computers become capable of breaking RSA and ECC encryption, is estimated leading academics at a 50:50 probability by 2031. Hybrid quantum-AI attack methods are compressing that timeline further.

> "Adversaries capturing encrypted traffic today do not need to decrypt it today. They only need patience."

Who is most at risk

- Financial services organisations carrying transaction records and client data with long-term regulatory retention requirements.
- Healthcare providers and NHS Trusts holding clinical records with decades-long sensitivity windows.
- Legal practices transmitting privileged communications and case documentation.
- Public sector and government bodies subject to NCSC guidance on post-quantum migration.
- Critical national infrastructure operators running fixed-function systems with long operational lifespans.
- Multi-site enterprises using IPSec or VPN-protected inter-site links across distributed networks.

The triggers that make this relevant now

Security framework or contract renewal approaching

Entering a renewal discussion without a clear post-quantum position creates unnecessary risk.

Regulatory readiness

NIST FIPS 203, 204, and 205 are published. The NCSC has issued migration guidance. Regulated organisations are expected to have a plan.

Legacy infrastructure with long operational lifespans

Systems that cannot be patched represent a persistent and growing HNDL exposure.

VMware exit planning

Following the Broadcom acquisition, many UK organisations reviewing VMware dependencies also face an opportunity to reassess the security model underneath their infrastructure.

Cloud repatriation

Returning workloads on-premise creates a natural opportunity to reset the cryptographic model at the same time.

NIST POST-QUANTUM STANDARDS

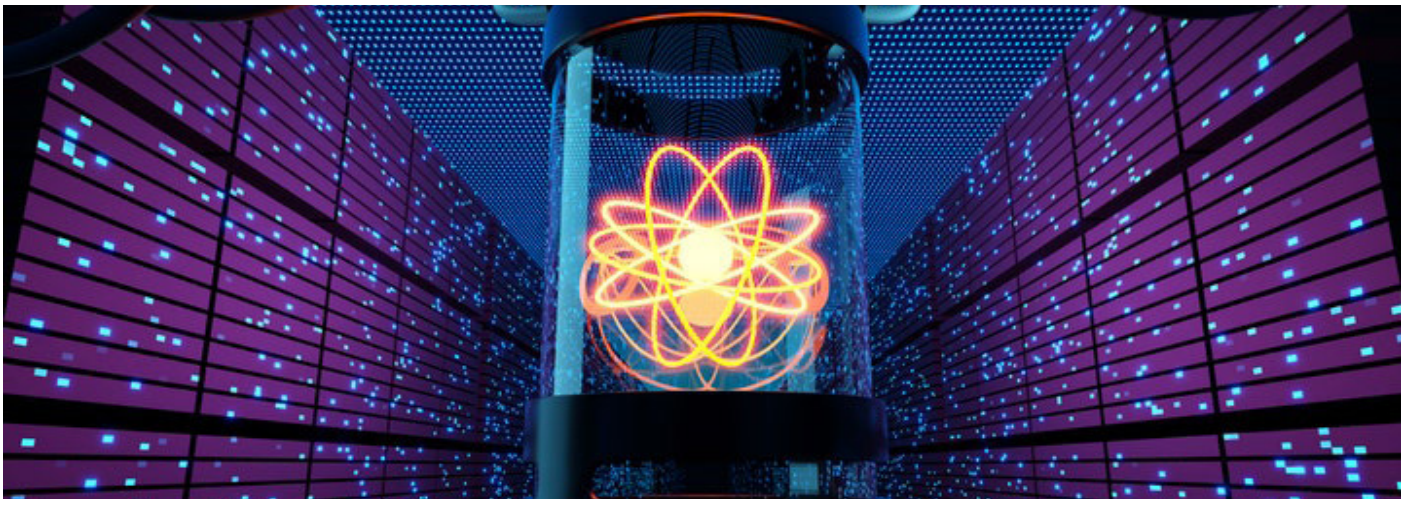
What NIST's post-quantum standards mean for UK organisations.

In 2024, the National Institute of Standards and Technology published its first finalised post-quantum cryptographic standards: FIPS 203, 204, and 205. This marked the end of post-quantum migration being optional for regulated organisations and government suppliers.

Standard	What it covers
FIPS 203	Lattice-based key encapsulation mechanism for key exchange.
FIPS 204	Lattice-based digital signature algorithm.
FIPS 205	Hash-based digital signature scheme.

Quantropi's QiSpace platform is aligned to NIST FIPS 203, 204, and 205. It is NATO-approved, benchmarked by

Deutsche Telekom, and recognised by the IEEE across multiple peer-reviewed publications. Recognised in the Deloitte Fast 50.



For IT Directors presenting a post-quantum response to their board or audit committee, NIST alignment is the credible foundation. It demonstrates that the approach is not proprietary or speculative. It is built on published, internationally recognised standards.

> "NIST's publication of FIPS 203, 204, and 205 confirmed that post-quantum migration is no longer a future consideration. It is a current-year compliance requirement for regulated organisations."

THE LEGACY GAP

Why not all systems can simply be upgraded.

Every enterprise IT estate contains systems that cannot be updated on demand. Industrial control platforms, fixed-firmware network appliances, clinical systems built on long-lifecycle architectures, embedded OT devices, and core financial platforms running IBM Power or legacy protocols cannot natively adopt post-quantum cryptographic standards.

These systems are not edge cases. They are active, data-carrying components of the network. And they represent a specific and persistent HNDL exposure precisely because they are the least likely to be upgraded on a timely basis.

Environments most affected

- Manufacturing and OT environments running industrial control systems with fixed firmware and multi-decade operational lifespans
- NHS Trusts and healthcare providers with clinical systems that cannot be patched at source.
- Utilities and critical national infrastructure operators running SCADA and fixed-function appliances.
- Financial services organisations with IBM Power-based core platforms running applications with decade-long lifecycles.
- Legacy IoT and embedded devices lacking the compute resources to run native NIST PQC algorithms.

The solution is not to replace these systems before they are due for replacement. It is to apply quantum-safe protection at the boundary, between the legacy system and the untrusted network, without touching the underlying device.

SOLUTION 1

Digital QKD: how it works, who it is for, and the key benefits.

The weakness at the heart of most enterprise encryption is not the algorithm. It is the key exchange.

Traditional key distribution protocols, IKEv2 and PKI, transmit cryptographic keys over the same network path as the data they protect. An adversary who captures that traffic today captures the keys alongside it. When quantum capability matures, decryption is straightforward.

Digital Quantum Key Distribution, D-QKD, powered by Quantropi's QiSpace platform and its Quantum Permutation Pad technology, eliminates this exposure entirely. Keys are derived independently at each endpoint and are never transmitted over the data path. An adversary who captures every packet in transit has nothing they can use, now or in the future.

D-QKD runs entirely in software over any IP network. No dark fibre. No photonic hardware. No distance limitations.

Benchmarked by Deutsche Telekom at over 250x faster than traditional optical QKD distribution rates.

Key benefits

- Software-defined deployment over any IP network. No dark fibre, no photonic hardware, no distance limitations.
- Keys never transmitted over the data path. HNDL exposure eliminated at the point of key exchange.
- Benchmarked by Deutsche Telekom at over 250x faster than photonic QKD distribution rates.
- Compliant with ETSI GS QKD 014
- Native integration with Cisco, Palo Alto Networks, Juniper, Fortinet, Ciena, and Ribbon Communications.
- Aligned to NIST FIPS 203, 204, and 205.

Best suited to

Financial services, legal, healthcare, public sector, and multi-site enterprises using IPSec or VPN-protected inter-site links where long-term data sensitivity creates HNDL exposure.

The outcome is not simply lower cost. It is a more controlled, more defensible cryptographic posture across your estate.

SOLUTION 2

Quantum-safe forward proxy: how it works, who it is for, and the key benefits.

Where D-QKD addresses the key distribution problem for modern infrastructure, the quantum-safe forward proxy addresses the harder problem: the substantial portion of every enterprise estate that cannot be re-engineered.

The proxy operates as an intermediary layer in front of existing legacy systems. It intercepts outbound traffic that would otherwise cross untrusted networks under classical encryption, re-encrypts it using Quantropi's TrUE suite of quantum-safe algorithms, and passes it on transparently to the receiving end. The underlying legacy system is unaware anything has changed. No modification to the source device. No downtime. No replacement programme required.

How it works

- Distributes quantum-generated entropy out-of-band to establish post-quantum pre-shared keys on legacy firewalls and IPSec VPN devices, without touching the data path.
- Post-quantum asymmetric encryption with smaller signature sizes, compatible with memory-restricted legacy processors.
- Quantum-secure symmetric encryption benchmarked at up to 18x faster than AES-256, with a latency profile legacy hardware can handle without performance degradation.

Key benefits

- No modification required to underlying legacy systems or devices.
- Quantum-safe re-encryption applied at the boundary before traffic crosses untrusted networks.
- Out-of-band key distribution via SEQUR on legacy firewalls and IPSec VPN devices.
- QEEP encryption benchmarked at up to 18x faster than AES-256.
- MASQ compatible with memory-restricted legacy processors.
- HNDL exposure eliminated without waiting for hardware refresh cycles.

Best suited to

NHS Trusts, manufacturing and OT environments, utilities, critical national infrastructure operators, industrial control system environments, and financial services or IBM Power platforms running applications with decade-long lifecycles.

ABOUT QUANTROPI

Award-winning quantum security platform.

Quantropi is a Canadian deep-tech company founded in Ottawa in 2018. Its QiSpace platform is the only end-to-end quantum security SaaS solution combining post-quantum asymmetric encryption (MASQ), quantum-secure symmetric encryption (QEEP), and quantum entropy distribution (SEQUR) in a single deployable solution.

Quantropi credentials

NATO-approved supplier	Quantropi is a NATO-approved vendor.
Deutsche Telekom benchmarked	Open QKD Lab. 250x faster than photonic QKD.
IEEE-recognised	Research published across peer-reviewed journals.
Deloitte Fast 50 awarded	Independent recognition of commercial credibility.
NIST FIPS 203, 204, 205	Aligned to published post-quantum standards.

ABOUT COVENCO

Infrastructure and managed services expertise since 1989.

Covenco has been securing critical IT infrastructure for UK organisations for over 35 years. We provide data management, backup and recovery, managed services, IBM infrastructure, and IT hardware supply and support across financial services, healthcare, manufacturing, public sector, and critical national infrastructure.

We are an IBM Gold Business Partner, ISO27001 certified, and Cyber Essentials accredited. Our UK data centres have over two petabytes of customer data under management. Our role in this partnership is to translate the QiSpace platform into a practical, supported deployment within your existing estate. You do not need specialist quantum expertise in-house. We provide it.

NEXT STEPS

How to assess your current exposure and begin a conversation.

A Quantum Encryption Assessment with Covenco and Quantropi establishes a clear picture of your current cryptographic exposure across modern and legacy infrastructure. It requires minimal effort from your team, carries no obligation beyond the initial engagement, and delivers a clear view of your HNDL exposure and the options available to address it.

If no material exposure is identified, the assessment provides documented assurance. If exposure is found, you will receive a clear proposal with a practical and achievable path to quantum-safe readiness.

Talk to us about your quantum encryption assessment:

Call: +44 (0)1753 732 000

Email: enquiries@covenco.com

About Covenco

Covenco connects data management services with IT hardware supply and support. With over 35 years of experience in the IT industry, our team offers a reliable source of expertise for data centre administrators.

Covenco supports businesses with world-class data protection, backup, and disaster recovery services.

Our UK data centres have over two Petabytes of customer data under management at any time, and we are fully ISO27001 accredited for data security.

Contact Covenco

Covenco UK Ltd Head Office
Unit 4, MXL Centre, Lombard Way,
Banbury, Oxfordshire. OX16 4TJ
United Kingdom

Telephone: +44 (0)1753 732000
Email: enquiries@covenco.com
https://covenco.com

COVENCO
DATA MANAGEMENT & INFRASTRUCTURE 365

veeam Cloud & Service Provider Platinum

IBM Gold Partner