WHITEPAPER

Harvest Now, Decrypt Later

The quantum threat that matters most isn't a future event — it's a present one. Understanding why long-lived sensitive data is already exposed, regardless of when quantum computers actually arrive.

A Breach With No Alarm

Most security incidents announce themselves: a system goes down, a login fails, an alert fires. "Harvest now, decrypt later" doesn't work that way. An adversary intercepts encrypted traffic or exfiltrates encrypted data today, stores it, and does nothing else. No decryption happens at the time of capture. There is no alarm to trigger, no anomaly to detect, because nothing that looks like a breach has actually occurred yet — only a quiet copy has been made.

The decryption step is deferred until a sufficiently capable quantum computer exists to break the algorithm that was used. At that point, the stored data becomes readable retroactively — including everything it protected on the day it was captured, however long ago that was.

Why Classical Public-Key Cryptography Is the Target

Widely used public-key algorithms — RSA, Diffie-Hellman, and elliptic-curve cryptography (ECC) — derive their security from mathematical problems that are extremely hard for classical computers to solve efficiently: factoring large numbers, or computing discrete logarithms. Quantum algorithms, most notably Shor's algorithm, can solve exactly these problems efficiently on a sufficiently large, error-corrected quantum computer. That's the specific reason RSA, Diffie-Hellman, and ECC are considered quantum-vulnerable, while, for example, well-implemented symmetric encryption (like AES) is far more resilient and only requires larger key sizes, not a different algorithm family.

This is precisely why the NIST post-quantum standards focus on replacing public-key operations — key establishment (ML-KEM, FIPS 203) and digital signatures (ML-DSA and SLH-DSA, FIPS 204 and 205) — rather than symmetric cryptography generally.

The Exposure Clock Started Long Before "Q-Day"

The industry shorthand for the point at which quantum computers become capable of breaking current public-key cryptography is sometimes called “Q-Day.” Precisely dating it is genuinely uncertain, and organisations that wait for a confirmed date before acting are optimising for the wrong variable.

The variable that actually matters is data longevity: how long does a given piece of data need to remain confidential? If that duration extends past a plausible Q-Day window — and for most regulated data, it does — then the relevant exposure has already begun, at the moment of capture, not at the moment of decryption. Waiting for certainty about the date doesn’t reduce the risk; it just delays the response to a risk that’s already accruing.

How Long Does Your Data Actually Need to Stay Confidential?

Different data types carry very different confidentiality windows, and those windows determine urgency far more precisely than any industry-wide timeline:

- Financial services — account, transaction and KYC records routinely require confidentiality across decades.
- Healthcare — patient records frequently require protection for the patient’s lifetime.
- Government and defence — classified information can require confidentiality for fifty years or more.
- Intellectual property — trade secrets and R&D data often need protection for as long as the product line exists.

Any of this data encrypted today with a quantum-vulnerable algorithm is a candidate for harvesting right now, whether or not an adversary has actually done so. The absence of evidence isn’t evidence of absence — passive interception, by design, leaves nothing to find.

What Actually Reduces This Exposure

There is no way to retroactively protect data that has already been harvested under a vulnerable algorithm. The only lever available is reducing how much new and currently-flowing data remains exposed, as quickly as realistically possible, prioritised by data longevity and business sensitivity rather than by convenience or system age.

That prioritisation is impossible without first knowing where quantum-vulnerable cryptography is actually in use — which is why discovery and inventory (a CBOM) come

before migration planning, not after it, in a properly sequenced Enterprise Cryptographic Exposure Management programme.

Registered as a limited company in England and Wales under company number: 17317113. Registered office: 71-75 Shelton Street, Covent Garden, London, WC2H 9JQ, United Kingdom.