CERTES

Are You Ready For Quantum?
Your Attackers Are!

The biggest cybersecurity threat is already here, and most businesses are still pretending it's decades away.

It's closer than you think.

Post-Quantum Cryptography (PQC) is a real and accelerating force that is already rewriting the rules of cybersecurity, and exposing a fatal flaw in how most organizations protect their data.

The Reality

Quantum decryption isn't future science, it's a present threat.

Nation-states and advanced attackers are already harvesting encrypted data today to break it tomorrow.

Your data is already stolen; criminals are just waiting to unlock it.

'Harvest Now, Decrypt Later' is the name of their game and it's working

The Clock Has Already Started

Today — Sensitive data leaves your network every second. Legacy security defences still in place.

+1 Year — Attackers harvest sensitive data: intellectual property, financials, customer PII. You can't detect it.

+2 Years — Your data is archived in threat actor repositories, waiting for the quantum era to strike.

+3 Years — Quantum computing advances. Standard encryption starts to break.

Quantum Day Zero — Your historical data is decrypted. Regulatory violations triggered. Trust destroyed. **No warnings given.**

If your data protection plan isn't quantum-safe now, your business and reputation won't survive this timeline.

The Numbers Don't Lie

62% — 62% of technology and cybersecurity professionals fear that quantum computing could break current internet encryption standards, but only 5% have a defined strategy in place

93% — Phishing cyber-crime is extremely prevalent: 93% of UK businesses that experienced any cyber-crime reported phishing.
Source: UK Government Cyber Security Breaches Survey 2025

$10.22m — Average cost of a data breach surged 9% in the United States to $10.22 million. Due to higher regulatory fines and detection/escalation costs.
Source: Secureframe

+50% — More than 50% of all breaches involve customer PII (personal identifiable information). Includes tax IDs, emails, phone numbers, and addresses.
Source: Secureframe

Still Think You Have Time?

Certes solves the PQC challenge.

Post-Quantum Protection Built-In
Certes DPRM (Data Protection & Risk Mitigation) integrates quantum-safe algorithms approved by NIST.

Protect the Data Itself
We don't rely on the perimeter. Even if attackers get in, they get nothing usable.

Compliance by Design
Full key ownership and audit-aligned controls support regulations including GDPR, DORA, NIS2, and CJIS.

Future-Proof Security
Certes protects your sensitive data today so it's not exposed five years from now when legacy encryption fails.

Zero Trust, Total Control. No Trust in the Network, Full Trust in the Data.

The breaches of 2029 have already begun in 2026.

The time to act is now.

Keep your data secret.
Keep your data Certes.

www.certes.ai