Transformativ IP

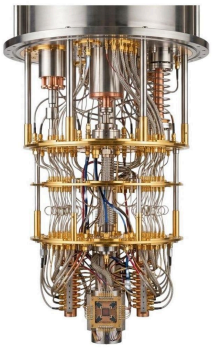
PQC+™

Overview of a 90-Day Path to Post-Quantum Resilience

Google, IBM, and Microsoft project that quantum capability will break the public-key encryption protecting roughly 95% of the global economy by 2029. The question is no longer *whether* to move to post-quantum cryptography. It is whether you move in time to withstand legal and regulatory scrutiny — and to keep the C-suite out of personal liability. Every encrypted record you hold today — patient or client files, financial data, IP, communications — is now being harvested by adversaries who plan to decrypt it in 2029.

Why Your Status Quo Fails

- **Two-front attack chain.** The swarm of AI bots are already a force multiplying harvester, scanning for weak implementations and quickly exfiltrating data. Quantum is the decryptor — Shor's algorithm collapses RSA/ECC from "lifetime of the universe" to minutes. Google's self-correcting Willow chip suggests that physics has been solved and that the problem is now engineering.
- **"Harvest Now, Decrypt Later" is active.** Long-lifespan data (health, financial, IP, defense) has a defined expiration date on its confidentiality. The clock started years ago.
- **An algorithm swap is not a strategy.** Replacing RSA or ECC with a NIST-approved PQC algorithm leaves the underlying architecture exposed: centralized key vaults remain a single point of failure, static long-lived keys turn one breach into years of stockpiled exposure, and external ACLs don't travel with the data once it leaves the perimeter.



A Quantum Computer

- **Lattice-based PQC strains legacy systems.** Many schemes introduce data bloat and latency that OT, ICS, and mainframe environments cannot absorb without re-engineering. That is time-consuming, error-prone, and a massive time waster. Most CTOs and CISOs are overworked.
- **The personal-liability math has changed.** Under the Learned Hand standard, a leader is negligent when the burden of prevention is less than probability × magnitude of harm. $B < (P * L)$. With prevention now a ~90-day software deployment, rising HNDL probability, regulatory compliance complexity, and effectively infinite loss magnitude, the math has flipped against inaction. Once a CTO or CISO flags the risk, the legal clock on the CEO starts running.

Why PQC+™ Is the Recommended Solution

PQC+ moves security out of the perimeter and into the data itself. It is 100% software, deploys in roughly 90 days with no rip-and-replace, and ships with two integration paths so brownfield and greenfield estates are covered without downtime:

- **SDK integration (greenfield):** embed libraries directly for field-level encryption and microservice ACLs — core operations in two lines of code.
- **Transport-layer protection (brownfield):** drop-in gateway transparently PQC-encrypts the data stream before it touches the network. Legacy OT, ICS, mainframes, and edge devices are protected with zero application changes.

It is built on NIST-standardized ML-KEM 1024 and ML-DSA 87, with a clear upgrade path to 2048 (US military), 5012, and 10240 (NSA and CIA) . Throughput runs near wire-line speed (~106 MB/s, 11 µs per packet) and operates inside relational databases in real time. PQC+ is the only post-quantum-strength software carrying DoD Impact Level 5, alongside FIPS 140-3, FDA, and DHS approvals.

PQC+'s Two Components and Why They Matter

Q-SecurKey™ — eliminates the static key target

- **No keys are ever stored.** Decryption keys are derived on demand from verified attributes (identity, clearance, location, time, zero-trust token) plus secret seeds and public parameters.
- **Session-only existence.** Each key lives for a single transaction and ceases to exist after — there is no vault to breach and no long-term secret for an HNDL attacker to wait on.
- **Removes the highest-value target in your stack.** Centralized KMS/HSM compromises become structurally impossible because there is nothing centralized to compromise.

Q-InfoSecur™ — embeds authorization inside the data

- **Self-enforcing data.** The access-control list is cryptographically bound to the encrypted payload. The data enforces its own rules wherever it travels — inside the perimeter or far outside it.
- **Instant revocation, no re-encryption.** Update policy and access changes immediately. No bulk re-encryption project, no downtime.
- **Multi-classification on a single system.** Top Secret through Unclassified can coexist on the same infrastructure, with the embedded ACL acting as a gatekeeper.

> ***Combined effect:*** *even if attackers obtain the ciphertext, they cannot decrypt it (PQC), cannot find keys (none stored), cannot brute-force it (AI-resistant), and cannot reach what they are not authorized for (embedded ACLs).*

PQC+ vs. Typical PQC Vendors

What Leadership Needs	Typical PQC Vendor	PQC+™
Time to deploy	Multi-year migration	~90 days, two lines of code
Hardware required	Yes — rip and replace	None — 100% software
Government certifications	Partial or none at PQ strength	FIPS 140-3, DoD IL5, FDA, DHS
Performance impact	Noticeable latency	Near wire-speed (~106 MB/s)
Free trial available?	Rare	Yes — fully functional trialware

The Decision in Front of You

Your mother told you to shop around — so do. When you do, the comparison is short: PQC+ deploys in ~90 days, fully installed, with no rip-and-replace, the strongest certification stack on the market, and a fully functional free trial. Doing nothing means guaranteed exposure to HNDL and personal liability under federal and state regulations. Running the trial costs nothing, requires no hardware, deploys against your real environment, and produces a documented record that leadership acted on a known, foreseeable risk — exactly the evidence that satisfies the Learned Hand test.

The threat is real. The legal exposure is personal. The remedy is unusually cheap. The only question is whether you start the trial this quarter or explain later why you didn't.

Transformativ IP

Regulatory Compliance + HNDL Protection
Federal & 50 States in 90 Days

Info@TransformativIP.ai
www.TransformativIP.ai

PQC+™