4QUAYS CRYPTO AGILITY FOR PQC MIGRATION

Quantum-safe. The enterprise's way.

Regulators have set the dates, and attackers are already harvesting encrypted data. 4Quays moves your enterprise to post-quantum **cryptography as a service by policy,** cutting the cost, time and risk of the largest cryptographic change in decades.

Lower cost | Regulator-ready | No rip and replace

MIGRATION APPROACH	TRADITIONAL	WITH 4QUAYS
Timeline	Multi-year[5]	Staged by policy
Who does it	Every app team	One platform team
Cost driver	Every system	One integration
Next algorithm	Another program	A policy edit
Audit evidence	Manual	Continuous

WHAT'S AT STAKE

The deadlines are set. The exposure is already here.

Data encrypted today can be stolen now and decrypted once quantum computers mature. Anything that must stay confidential past 2030 is already at risk.

$4.99M[1]

Average cost of a data breach

Global average in 2026, rising to $11.5M in the United States.

2030[2,3]

High-risk systems must migrate

EU deadline for finance, energy, health and transport. NIST deprecates RSA and ECC the same year.

2%[4]

Of global turnover

Maximum NIS2 fine for essential entities, or €10M if higher.

WHAT THE BUSINESS GETS

Lower risk, lower cost. Less time.

4Quays turns post-quantum migration and operations from vendor control into an enterprise capability that your operations and security teams can agree on.

01

Reduce risk

Protect your most sensitive, longest-lived data first, ranked by business impact.

02

Contain cost

No rip and replace, no scarce PQC hires. One integration instead of a rewrite per system.

03

Move faster

Algorithm changes become policy decisions rolled out across the estate, not projects.

04

Prove compliance

Board- and regulator-ready evidence of progress, continuously, in tools you already use.

0

Application rewrites

Quantum-safe uplift inside the systems and investments you keep.

1

Integration, every future algorithm

PQC is one transition, not the last. The next is a policy edit.

100%

Of cryptographic operations on record

Every change is evidenced for auditors, regulators and the board.

HOW IT WORKS

Implement and integrate once. Change through policy.

One integration turns cryptography into a governed, upgradable service. Every algorithm after that is a central policy decision. And change management has a check and balance.

Observe
Discover cloud, code and network assets, or import a CycloneDX CBOM.

Execute
Apps call protect / unprotect. No keys in the app, no per-algorithm work.

Govern
Classical, hybrid or PQC per policy, versioned and staged with rollback.

Prove
Every operation audited, with alerts on drift and evidence in your SIEM.

Live crypto inventory (CBOM)
Discover keys, certificates and algorithms, or import CycloneDX with AI-assisted parsing, then export.

Risk-ranked migration backlog
Scored against NIST SP 800-57 and 800-131A, with vendor readiness from qIntel (powered by Quantanaut).

Hybrid classical + post-quantum
Run classical and PQC side by side, interoperating with partners who haven't moved yet.

Staged, reversible rollout
Versioned policies, live observability and controlled rollback. No cut-over is a one-way door.

Key lifecycle & rotation
Generate, rotate and retire keys under policy, including destination-managed keys held by the receiving party.

4Q Agent, your cryptographic expert
Ask what's vulnerable and what to migrate first. It explains, never executes, and signs its answers.

Common platform

INCLUDED IN EVERY 4QUAYS DEPLOYMENT

Discovery
Cloud KMS, code, network, endpoints and AI agents.

Prioritization
Risk scoring against NIST guidance and vendor readiness.

Monitoring
Latency, error rate, throughput and volume per policy.

Alerting
Threshold, drift and missing-activity rules.

Auditing
Every operation, with policy, algorithm and key.

SIEM & logging
Monitoring, audit and alert data to your SIEM.

TECHNICAL SPECIFICATIONS

Post-quantum	ML-KEM-512 / 768 / 1024 (FIPS 203) · ML-DSA-44 / 65 / 87 (FIPS 204) · classical, hybrid or PQC per policy
Classical	AES-128/192/256-GCM (FIPS 197) · RSA-2048/4096 · ECDSA P-256/P-384 (FIPS 186-5) · SHA-2
SIEM & logging	Splunk · Sentinel · Datadog · Elastic · QRadar · Sumo Logic · Falcon LogScale · webhook
Integration	REST API · `@4quays/sdk` (TypeScript) · `@4quays/mcp` for AI assistants
Standards alignment	NIST FIPS 203 / 204 · NIST SP 800-57, 800-131A · CNSA 2.0 · NIS2 · EU Cyber Resilience Act

1. IBM Security & Ponemon Institute, *Cost of a Data Breach Report 2026*.
2. NIS Cooperation Group, *Coordinated Implementation Roadmap for the Transition to PQC*, 2025.
3. NIST IR 8547 (initial public draft), *Transition to Post-Quantum Cryptography Standards*, Nov 2024.
4. Directive (EU) 2022/2555 (NIS2), Article 34.
5. NIST NCCoE SP 1800-38, *Migration to PQC*: past migrations such as SHA-1 took years, some over a decade.

SEE IT LIVE

See 4Quays change cryptography in a live environment.

Book a demo

contact@4quays.com
4quays.com