THE CRYPTO-AGILITY CONTROL PLANE

# Agile digital trust for quantum and AI.

Quantum computing will break the cryptography your business runs on, and AI agents now act with your keys at machine speed. 4Quays lets you change that cryptography **by policy, not by rebuild,** across applications, connections and AI agents, at a fraction of the cost and time.

Lower risk | Lower cost | Regulator-ready

| ENTERPRISE CRYPTOGRAPHY | TODAY | 4QUAYS |
|---|---|---|
| Visibility | Partial, stale | Live inventory |
| Who does it | Every team | One platform |
| Next algorithm | A new program | A policy edit |
| AI agents | Ungoverned | Signed, governed |
| Audit evidence | By hand | Continuous |

WHAT'S AT STAKE

## Two forces. One deadline.

Quantum risk and AI agents both demand cryptography that can change quickly. Most vendors built their cryptography never to change at all.

**$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 post-quantum migration. NIST deprecates RSA and ECC the same year.

**25%**[4]

### Of enterprise breaches

Traced to AI agent abuse by 2028, by outsiders and insiders alike.

ONE PLATFORM, FIVE OUTCOMES

## One investment. Every place cryptography lives.

Applications, connections and AI agents share the same discovery, policy, keys and evidence, so each use case pays for the next, at machine speed with learning.

01

### PQC Migration

Quantum-safe without rewriting every application or running a multi-year program.

02

### AI Verification

Prove what every agent said and did, to auditors, partners and customers.

03

### AI Security

Keep agents in bounds and contain incidents without shutting AI down.

04

### Machine-to-Machine

One decision reaches every connection, in hours, with no vendor lock-in.

05

### Threat Detection

Threats and issues detected at machine speed, with learning.

**5**

### Standards bodies

Where the team holds seats, including the NIST NCCoE PQC project.

**24/7**

### Security operations

Run at national scale, for dozens of federal departments.

**3**

### ISO regimes

Previous environments operated under ISO 27001, 27017 and 27018.

HOW IT WORKS

# Implement and integrate once. Change through policy.

One integration turns cryptography into a governed, upgradable service. After that, teams don't implement each new algorithm.

### Observe
A live inventory (CBOM) of keys, algorithms, services, connections and AI agents, risk-ranked.

### Execute
Protect, sign and encrypt through API, SDK, MCP and hooks. No keys in apps or prompts.

### Govern
Algorithms, keys, providers, channels and envelopes set centrally, staged and reversible.

### Prove
Every operation audited, public signature checks, alerts on drift, evidence in your SIEM.

### Policy-driven change
Decide centrally, then apply with visibility and controls.

### Staged and reversible
Hybrid adoption, live observability and controlled rollback.

### Ready for what is next
Algorithm changes become operations, not vendor-dependent multi-year programs.

## 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

| | |
|---|---|
| **Algorithms** | ML-KEM (FIPS 203) · ML-DSA (FIPS 204) · AES-GCM · RSA · ECDSA · classical, hybrid or PQC per policy |
| **Discovery sources** | Azure Key Vault · AWS KMS/ACM/Secrets Manager · GCP KMS · GitHub · Bitbucket · Cloudflare · Zeek · Defender · FleetDM · Qualys · CycloneDX |
| **AI agent discovery** | AWS Bedrock Agents · OpenAI Agents · Azure AI & Entra Agent ID · frameworks in source |
| **SIEM & logging** | Splunk · Sentinel · Datadog · Elastic · QRadar · Sumo Logic · Falcon LogScale · webhook |
| **Integration** | REST API · `@4quays/sdk` · `@4quays/mcp` · signing hooks · `4q` CLI · gateways |
| **Standards alignment** | NIST FIPS 203 / 204 · SP 800-57, 800-131A · CNSA 2.0 · NIS2 · EU Cyber Resilience Act · EU AI Act |

1. IBM Security & Ponemon Institute, *Cost of a Data Breach Report 2026*.
2. NIS Cooperation Group, *A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography*, June 2025.
3. NIST IR 8547 (initial public draft), *Transition to Post-Quantum Cryptography Standards*, Nov 2024.
4. Gartner, *Top Strategic Predictions for 2025 and Beyond*, Oct 2024.

SEE IT LIVE

## See 4Quays change cryptography in a live environment.

Book a demo

contact@4quays.com
4quays.com