AGILE TRUST INFRASTRUCTURE FOR THE ENTERPRISE

Your risk. Your trust layer.

The enterprise, not its vendors, bears the consequences of a breach, yet vendors embed the math behind its trust in every application, device and entry point. 4Quays gives you **central control, visibility and policy over that trust,** for you and your digital partners, whatever the technology.

Fix forward once | No rip and replace | Cloud, hybrid, on-prem

TRUST INFRASTRUCTURE	TODAY	WITH 4QUAYS
Who controls it	Each vendor	The enterprise
Visibility	Fragmented	Central, fine-grained
Next algorithm	Rip and replace	A policy change
AI agents	Self-policing	Under your policy
Trading partners	Their standards	Your standards

WHAT'S AT STAKE

The landscape keeps growing. Its math is under threat.

BYOD and remote work stretched the landscape to protect. Now AI and quantum computing threaten the cryptography it stands on.

$4.99M[1]

Average cost of a data breach

Global average in 2026, carried by the enterprise, not its vendors.

82:1[2]

Machine identities per human

Each one a vendor's embedded trust decision that someone must protect.

2030[3]

RSA and ECC deprecated

NIST's date for retiring the math most enterprise trust runs on today.

AI is an accelerant. It's as if you once had 30 super admins over 30 applications and 30 data warehouses, and now you have one super admin who is not on your payroll.

WHAT THE BUSINESS GETS

AI and quantum safe. Without crowding out innovation.

An agile service layer cuts the time, cost and risk of the move, and uplifts run-time controls to machine speed.

01

Agency over trust

Central policy and visibility for cryptography and AI, held by the enterprise.

02

Uplift, don't replace

Keep current and future investments. No rip and replace for math.

03

Partner alignment

Exchanges with trading partners held to your security standards.

04

Vendor portability

Trust lives in your layer, not each product, so vendors are easier to change.

1

Fix forward, once

Faster, cheaper and better than a program per algorithm or vendor.

0

Rip and replace

Aligned to your vendors' roadmaps and the upgrades they ship.

3

Deployment models

Cloud, hybrid and on-prem, under one set of policies.

WHY WE BUILT IT THIS WAY

Control is an outcome. The enterprise should own it.

In cybernetics, control comes from corralling all the inputs that create your operating environment. That is hard when every vendor brings its own math, controls and requests for change, while the enterprise and its stakeholders bear the risk.

AI is an accelerant, running exploits at low cost across environments static software never could. So we designed for **enterprise agency over AI security,** as over its own cryptography, beyond whatever AI may do to constrain itself.

ONE ARCHITECTURE, EXTENSIBLE BY DESIGN

The layer that keeps your math agile also puts AI under your control.

The math of digital trust

As trust migrates to quantum-safe variants and runs on them. There will be many maths, so the engine stays evergreen.

Classical · Hybrid · Quantum-safe

AI across your whole enterprise

Control and visibility over how AI runs, for your people, your digital assets and your agents.

When · How · Where · For whom

Agile trust architecture · central, fine-grained policy and visibility · at machine speed

WHEN A BOUNDARY IS CROSSED

Two responses anyone can understand.

Kill memory

What it has built up is sealed, so it can't carry on from it.

Kill purpose

Reach and permissions are withdrawn, so the task goes nowhere.

Your policies set the boundaries, as finely as you need, and defences activate at machine speed.

WHEN A VENDOR ASKS FOR MORE

Every change, on your terms.

01 **A change is requested** to access or entitlements.

02 **You're alerted in real time,** inside your security operations.

03 **It's actioned against policy** for your consideration.

04 **The enterprise decides.** Always.

If every vendor can prompt your team directly, they get overwhelmed, and well-meant decisions become ones they regret.

Built for run time. If it doesn't work in run time, we aren't adding value. We're adding an expense.

KEY FEATURES

- ✓ Agile, evergreen math engine
- ✓ Central, fine-grained policy enforcement
- ✓ Central, fine-grained visibility
- ✓ AI and quantum-safe identity
- ✓ Pair-wise transaction flexibility
- ✓ Uplifts current and future investments
- ✓ Cloud, hybrid and on-prem
- ✓ Ingests CBOM and discovery tools
- ✓ Aligned to future vendor roadmaps
- ✓ Integrates with SOC, SIEM and MDR
- ✓ Increases vendor portability

1. IBM Security & Ponemon Institute, *Cost of a Data Breach Report 2026*.
2. CyberArk, *2025 Identity Security Landscape*, Apr 2025.
3. NIST IR 8547 (initial public draft), *Transition to Post-Quantum Cryptography Standards*, Nov 2024.

FIX FORWARD ONCE

Faster, cheaper and better. See it in a live environment.

Book a demo

contact@4quays.com · 4quays.com