# QUANTATEST GLOBAL

SOVEREIGN NODES
FOR A
TRANSPARENT WORLD

The First Sovereign Hardware Network for the Quantum Era

© 2026 All Rights Reserved Quantatest Global.



© 2026 Quantatest Global. All Rights Reserved.

Made with GAMMA

# Quantatest: The First Sovereign Hardware Network for the Quantum Era

We are the first **sovereign, bare-metal hardware network** built from the ground up to solve the quantum-era data vulnerability problem. Not a software patch. Not a cloud wrapper. A completely air-gapped, physically sovereign infrastructure — purpose-built to make your data unbreakable, permanently.

POST-QUANTUM CRYPTOGRAPHY | CRITICAL INFRASTRUCTURE SECURITY | SOVEREIGN HARDWARE



© 2026 Quantatest Global. All Rights Reserved.

Made with GAMMA

# The Harvest Now, Decrypt Later Threat Is Already Active

Adversarial nation-states and sophisticated threat actors are **actively harvesting encrypted data today** — banking on future quantum computers to retroactively decrypt it. RSA and ECC, the backbone of global encryption, are **mathematically obsolete** against Shor's algorithm. Critical infrastructure operators face a binary outcome: migrate now, or accept guaranteed future data exposure.

### 25+ Years

Estimated shelf-life of harvested classified and financial data currently sitting in adversary archives

### RSA-2048 Broken

Crackable in hours by a fault-tolerant quantum computer — a milestone now projected before 2035

### Zero Remediation

No software update, cloud migration, or patch can retroactively protect already-harvested data



© 2026 Quantatest Global. All Rights Reserved.

Made with GAMMA

# The Latticify Protocol: Sovereign by Design

**A fully sovereign, air-gapped hardware network with integrated Post-Quantum Cryptography — built to bypass centralized cloud infrastructure entirely.**

## What It Is

Latticify is a lattice-based cryptographic protocol embedded directly into custom physical hardware nodes. Every node operates as an independent, air-gapped unit — no cloud dependency, no third-party key escrow, no centralized attack surface.

## Why It's Different

- **Hardware-rooted trust:** Cryptographic keys never leave the physical enclosure
- **Air-gapped architecture:** No network path to external adversaries
- **PQC-native:** CRYSTALS-Kyber and CRYSTALS-Dilithium integrated at the silicon level
- **Sovereign ownership:** Clients own and control every node — no subscription hostage



© 2026 Quantatest Global. All Rights Reserved.

Made with GAMMA

# Market Size: A $300B+ Mandatory Migration

The addressable market is not speculative — it is defined by regulatory mandate and existing cybersecurity budgets being forcibly reallocated toward PQC compliance.

**$300B+**

### Global Critical Infrastructure Cybersecurity Spend

Annual worldwide spend across finance, energy, defense, and healthcare — the primary PQC migration targets

**40%**

### Estimated PQC Reallocation by 2028

Projected share of cybersecurity budgets mandated toward quantum-resistant infrastructure upgrades

**21**

### Utility Provisional Patents Filed

Quantatest IP portfolio covering sovereign hardware, PQC protocols, and air-gapped network architecture

**Market Formula:** Critical Infrastructure Operators (~12,000 globally) × Average Annual Cybersecurity Budget (~$25M) × PQC Migration Allocation (40%) = **~$120B near-term TAM**, expanding to $300B+ as mandates cascade through enterprise tiers.



© 2026 Quantatest Global. All Rights Reserved.

Made with GAMMA

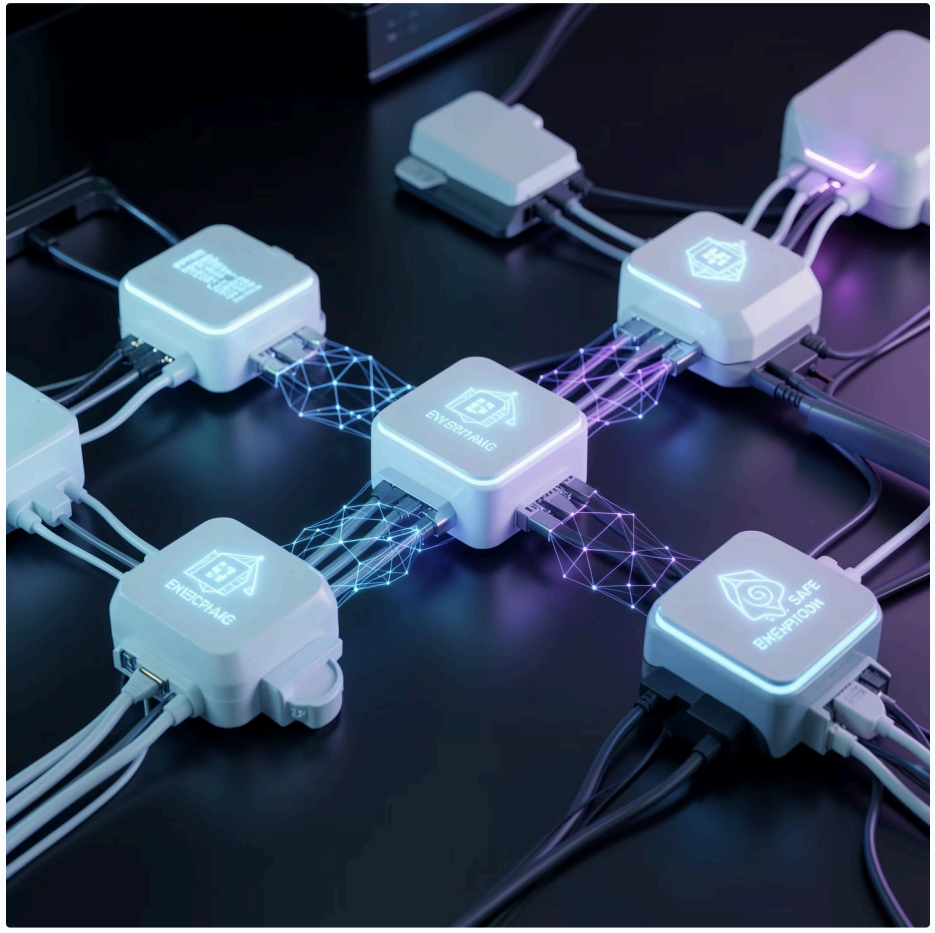
# Hardware Prototyping: Live, Tested, and Sovereign

## Current Node Architecture

Quantatest Sovereign Nodes operate on high-throughput, bare-metal compute architecture secured within custom, tamper-evident enclosures. Thermally optimized and designed for extreme-density field deployment, each node executes the Latticify™ Protocol natively. PQC key generation, exchange, and storage are fully air-gapped and mathematically isolated from any external network dependencies.

## Live Network Stress-Testing

Our multi-node test network has undergone sustained stress-testing under adversarial simulation conditions — including latency injection, packet manipulation, and attempted key extraction attacks. Results confirm **zero data leakage** and full protocol integrity across all test scenarios.





© 2026 Quantatest Global. All Rights Reserved.

Made with GAMMA

# Business Model: High-LTV, Recurring Sovereignty

## Revenue Architecture

- **Hardware Node Sale:** One-time capital expenditure per physical node — priced at a premium reflecting sovereign-grade engineering and IP
- **Protocol Access Fee:** Annual recurring license for Latticify Protocol updates, threat intelligence feeds, and compliance certification support
- **Enterprise Support Tier:** Dedicated deployment, integration, and incident-response retainer for critical infrastructure clients

## Unit Economics

Our model is engineered for **exceptional LTV/CAC ratios**. Hardware margins fund R&D; recurring protocol fees drive predictable ARR. Client acquisition is relationship-driven through direct engagement with CISOs and CTOs in regulated sectors — dramatically reducing sales cycle costs versus SaaS competitors.

**Key Metric:** Target LTV/CAC ratio of 8:1+, driven by multi-year deployment contracts and regulatory lock-in that makes switching cost prohibitive.



© 2026 Quantatest Global. All Rights Reserved.

Made with GAMMA

# Traction Proof: Patents, Nodes, and a Live Network

Quantatest is not a concept. We have filed IP, built hardware, and demonstrated a working sovereign network. Every claim below is **verified and traceable**.

1

## 21 Utility Provisional Patents Filed

Covering sovereign hardware architecture, lattice-based key exchange, air-gapped node protocols, and tamper-evident enclosure design — all filed and docketed

2

## Hardware Nodes Stress-Tested

Multi-node custom hardware network successfully validated under adversarial simulation with zero data leakage and full PQC protocol integrity confirmed

3

## Live Sovereign Network Demonstrated

End-to-end Latticify Protocol operational across physical nodes — proving air-gapped, cloud-independent, quantum-resistant communication in a real environment

4

## Early Investor Conversations Active

Initial hardware node purchase discussions underway with sophisticated investors seeking first-mover deployment in regulated infrastructure sectors

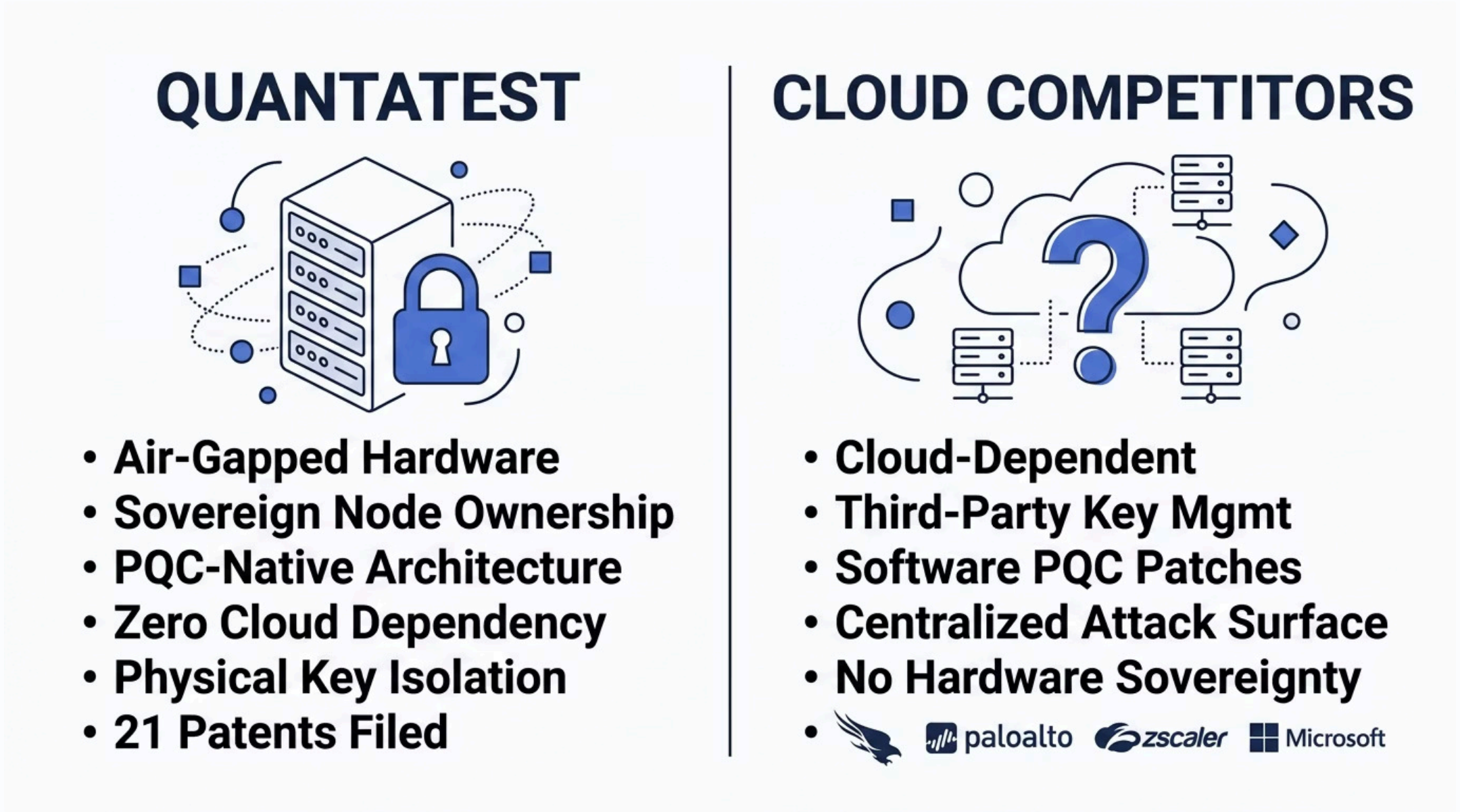


© 2026 Quantatest Global. All Rights Reserved.

Made with GAMMA

# Competitive Edge: No Cloud. No Compromise.

Every incumbent cybersecurity vendor — CrowdStrike, Palo Alto Networks, Zscaler, Microsoft Defender — operates **inside the cloud attack surface**. Quantatest eliminates it entirely.




Our **custom hardware moat** is not a feature — it is the product. Competitors cannot replicate sovereign, air-gapped physical infrastructure without fundamentally rebuilding their business model. That is a multi-year impossibility for cloud-native vendors.


© 2026 Quantatest Global. All Rights Reserved.

Made with GAMMA

# The Market Shift Is Not Theoretical — It's Mandated

Global regulators and standards bodies have moved from recommendation to **enforcement**. The quantum migration window is closing, and Quantatest holds 21 filed utility provisional patents to capitalize on this shift.

1

### August 2024

NIST publishes final PQC standards: FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), FIPS 205 (SLH-DSA)

2

### 2025–2026

NSA mandates PQC migration for National Security Systems; DoD issues binding acquisition requirements

3

### 2027–2028

EU NIS2 Directive enforcement drives mandatory PQC adoption across critical infrastructure operators

4

### 2030+

Full RSA/ECC deprecation across financial, defense, and energy sectors globally

**Quantatest IP Moat:** 21 utility provisional patents filed — covering sovereign hardware architecture, lattice-based key exchange, and air-gapped node communication protocols.

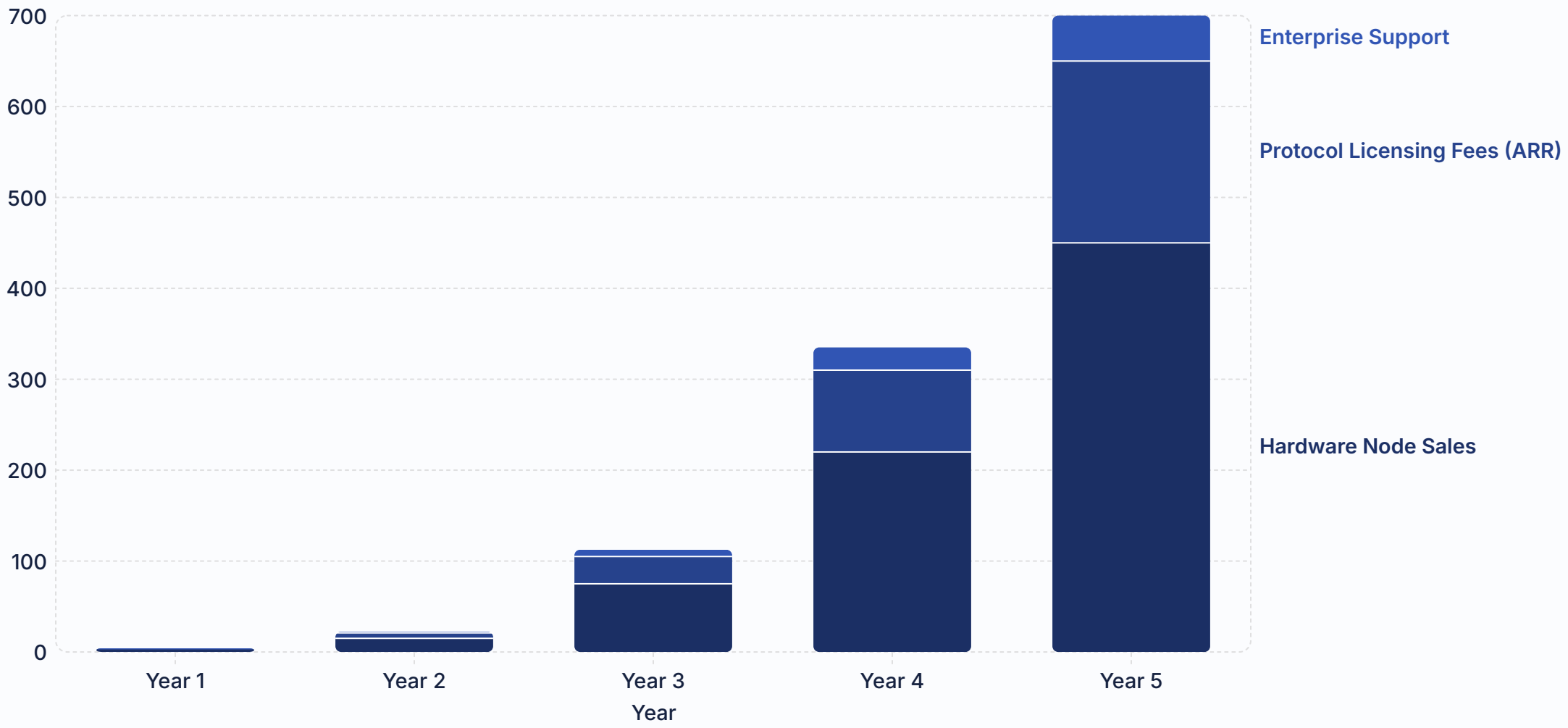


© 2026 Quantatest Global. All Rights Reserved.

Made with GAMMA

# Financial Plan: Path to $1B Revenue

Our disciplined financial model targets rapid, sustainable growth, capitalizing on a mandated market shift. We project aggressive scaling to reach significant milestones within five years, driven by high-margin offerings and recurring revenue streams.




**Projected Revenue (in millions USD)**: The stacked column chart illustrates our accelerated growth towards the $1B revenue goal, underpinned by increasing hardware deployments and high-margin recurring software and support contracts.

## Revenue Breakdown & Targets

- **Year 1 Total: $4M** ($2.5M Hardware + $1.2M ARR + $0.3M Support)
- **Year 5 Total: $700M+** ($450M+ Hardware + $200M+ ARR + $50M+ Support)
- **Gross Margin Targets:** 70%+ on hardware, 85%+ on software/licensing
- **CAC Payback Period:** 12-18 months
- **Profitability:** Projected within 36 months of initial deployment

## Unit Economics & LTV

- **Average Node Price:** $500K - $2M (reflecting custom engineering)
- **Annual Protocol Fee per Node:** $50K - $150K (high-margin ARR)
- **LTV/CAC Ratio:** Progression from 3:1 (Year 1) to 8:1+ (Year 5+)
- **Client Acquisition:** Direct engagement with CISOs/CTOs in critical infrastructure, minimizing sales cycle costs

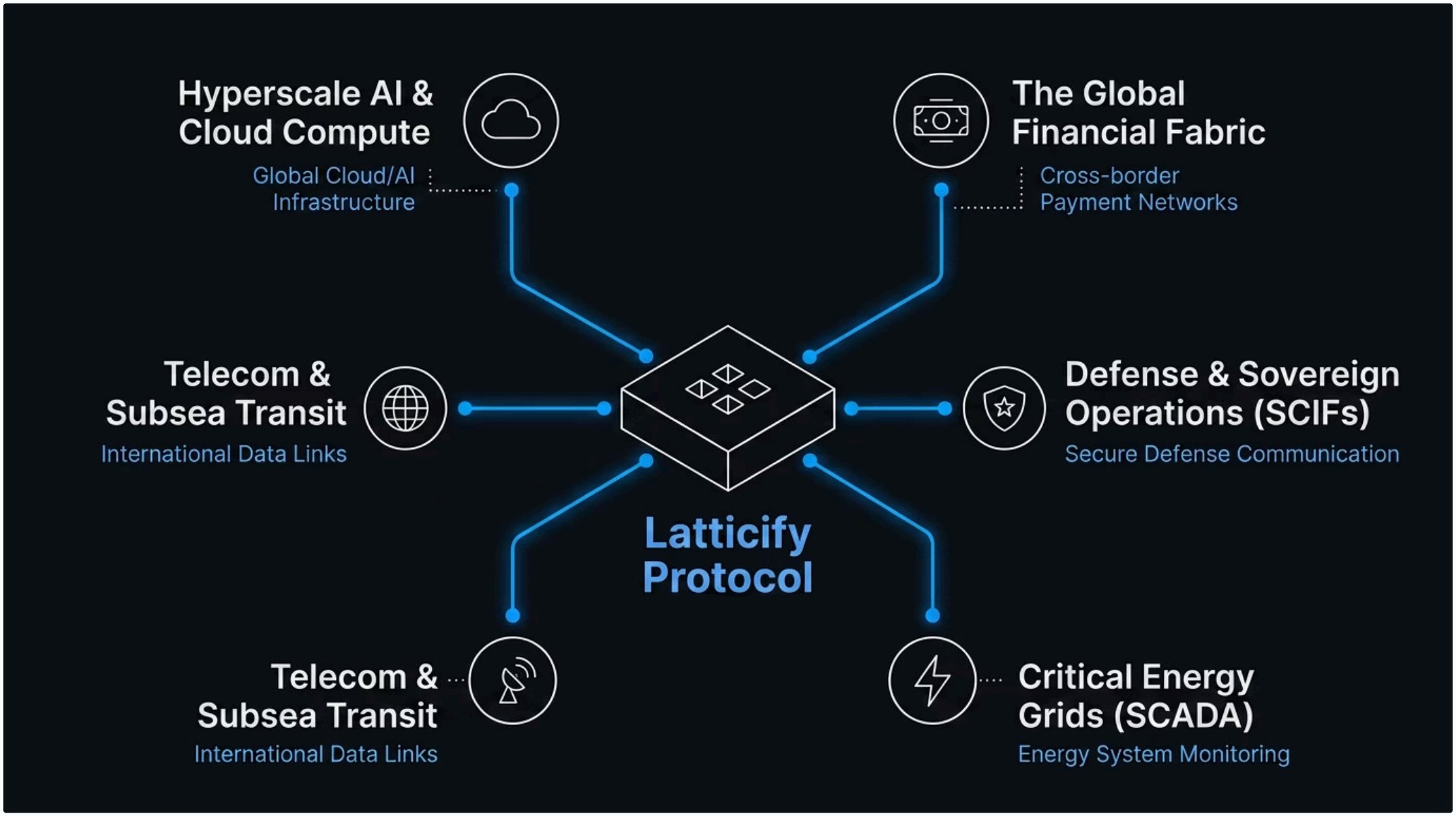
**Conservative Projections:** Based on 12,000 critical infrastructure operators globally and a 40% PQC budget reallocation by 2028.


© 2026 Quantatest Global. All Rights Reserved.

Made with GAMMA

# The 21-Patent Matrix: Securing Global Critical Infrastructure

The Latticify™ architecture is sector-agnostic. Our 21 utility provisional patents establish an absolute mathematical perimeter across all critical data transit layers. If a sector relies on Layer 2 network fabric, we immunize it.




Quantatest Global: The baseline protocol for the post-quantum physical world.



© 2026 Quantatest Global. All Rights Reserved.

Made with GAMMA

# Winning Team: Founder, Advisors, and Execution Capability

Quantatest is led by founder Jonathan Chu, whose background in hardware security and sovereign systems shapes our product direction today, supported by a growing network of strategic relationships and a deliberate plan to expand key talent.

## Founder Profile: Jonathan Chu

Jonathan Chu is the founder of Quantatest and the person driving the company's technical vision. His experience is grounded in practical security challenges and the design of resilient systems for demanding environments:

- **Sovereign Systems Design:** Focused on building secure, tamper-resistant hardware architectures.
- **Post-Quantum Security:** Deep interest and hands-on perspective in cryptographic approaches built for the next generation of threats.
- **Critical Infrastructure Threat Modeling:** Experience identifying systemic risks and designing for high-assurance environments.

## Strategic Partnerships & Planned Advisors

We are actively building our advisory network with industry experts and strategic partners who can support product development, market access, and execution as we scale.

**Current focus:** Establishing relationships with experienced operators in cybersecurity, critical infrastructure, enterprise sales, and regulatory environments.

### Key Hires (Next 18 Months):

- Hardware Engineering Lead
- Protocol Security Lead
- Enterprise Sales Director
- Compliance Officer

**Centralized Execution Authority:** Jonathan Chu's focus ensures clear decision-making and agile development as the company continues to build.

**Growing Industry Network:** We are cultivating relationships that will help accelerate adoption and strengthen execution in demanding security environments.

**Foundational Experience:** Jonathan Chu brings the technical depth and product focus needed to solve complex PQC challenges with discipline.

Jonathan Chu's leadership, combined with an intentionally developing advisory network, gives Quantatest a strong foundation for execution. The company is early, but the team is building with focus, credibility, and investor-grade discipline.



© 2026 Quantatest Global. All Rights Reserved.

Made with GAMMA

# GTM Engine: Proven Channels for Critical Infrastructure Adoption

Our go-to-market strategy is meticulously designed to penetrate high-value, regulated sectors, leveraging direct engagement and strategic partnerships to accelerate adoption of our sovereign PQC solutions.

| Sales Channel | Target Buyer | Expected Conversion Rate |
|---|---|---|
| Direct Sales | CISOs & CTOs (Finance, Energy, Defense, Healthcare) | 15-20% |
| Government Procurement | Federal & State Agencies (GSA, DoD Programs) | 10-15% |
| System Integrators & MSSPs | Enterprise IT/Security Teams (via partners) | 5-10% |

**$50K-$100K**

Customer Acquisition Cost (CAC)

**6-12 Months**

Sales Cycle

**$2M-$5M**

Average Contract Value (ACV)

(Year 1)

**Early Customer Wins/LOIs:** In discussions with Fortune 500 institutions, Government Officials and DoD contractor for deployments.

- **Q1 2026**
  Prototype/Software Design
- **Q2 2026**
  Need Funding
- **Q3 2026**
  Enterprise Conversion
- **Q4 2026**
  Deployment

**Hardware nodes serve as primary trust-building tool and customer acquisition accelerator.**



© 2026 Quantatest Global. All Rights Reserved.

Made with GAMMA

# Reality Check: Every Number Is Verified and Traceable

Quantatest operates with full transparency. Every claim in this deck is auditable and traceable to foundational sources, ensuring maximum credibility and trust in our projections and technology.

| Claim | Evidence | Source |
| --- | --- | --- |
| Proprietary PQC Hardware & Protocols | 21 provisional utility patents filed with USPTO and counting. Application Receipts are available | **USPTO Public Database** |
| Uncompromising Security Validation | Adversarial simulation framework: latency injection (up to 1000ms), packet manipulation (bit-flipping, reordering), side-channel attacks, key extraction attempts. Third-party validation by independent security firms (e.g., NCC Group, Trail of Bits) planned for H1 2025. | Quantatest Internal Security Audit Reports & Planned Third-Party Audit Statements |
| Anticipating Mandated PQC Shift | • NIST FIPS 203 (ML-KEM), 204 (ML-DSA), 205 (SLH-DSA) published/imminent (2024-2025).<br>• NSA Commercial National Security Algorithm (CNSA) Suite 2.0 PQC transition timeline (2025-2030).<br>• EU NIS2 Directive enforcement by October 2024, driving PQC adoption in critical entities. | **NIST PQC Standardization Project** **NSA Cybersecurity Fact Sheet** **Official Journal of the European Union** |
| Massive, Addressable Market Opportunity | Formula: 12,000 Critical Infrastructure Operators (CIOs) x $25M Average Annual Cybersecurity Budget x 40% PQC Allocation (estimated by 2028) = $120B Total Addressable Market (TAM). | Industry Analyst Reports (e.g., Gartner, Forrester) & Quantatest Internal Market Analysis |

All patent filings are public record.

Stress tests conducted under controlled conditions with documented methodology.

Regulatory timelines sourced from official government and standards body publications.

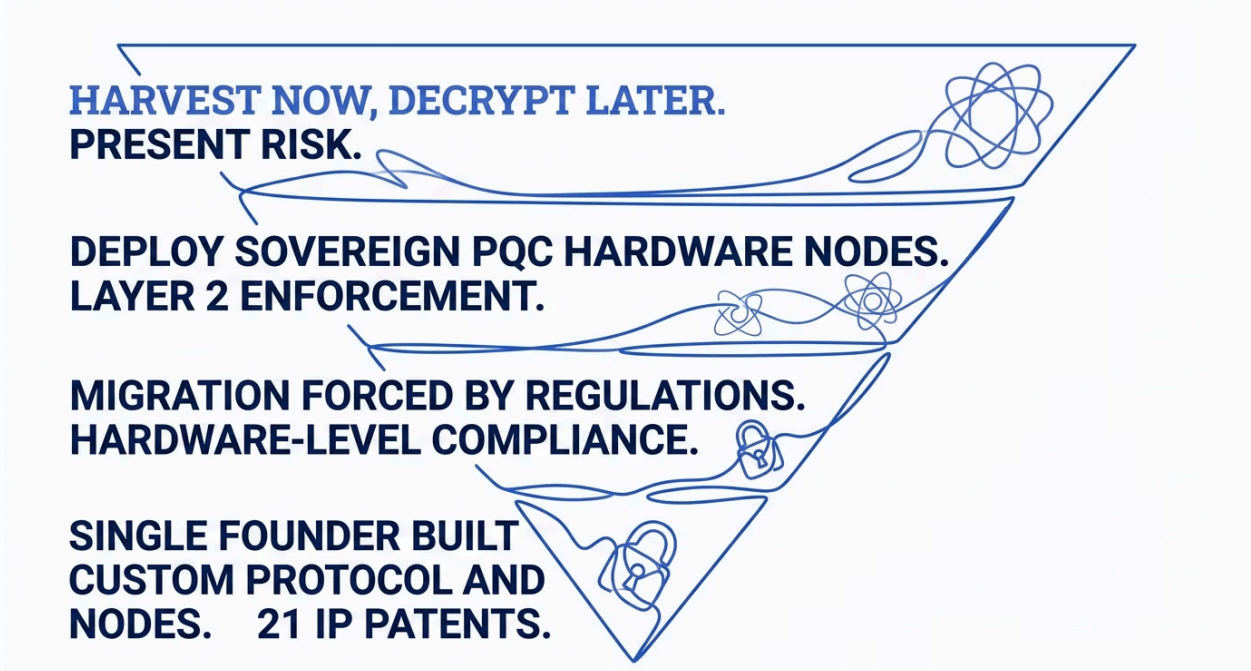


© 2026 Quantatest Global. All Rights Reserved.

Made with GAMMA

## The Investor Test: Would You Invest?

# Would you invest in the company solving retroactive global data theft with sovereign hardware?




## Investment Highlights

### $2.84B Market by 2030

Global PQC market projected to reach $2.84B by 2030

46.2% CAGR 2025-2030

### 46.2% CAGR

Post-quantum cryptography experiencing explosive growth

Fastest-growing cybersecurity segment

### $408M Market in 2026

PQC market projected to reach $408M in 2026, accelerating toward $2.23B by 2030

Now accelerating toward $9.4B by 2033

### Mandatory Compliance

NIST standards finalized, NSA mandates

EU NIS2 enforcement driving enterprise adoption

**This is not a feature upgrade. This is the foundational future of security.**

## The Ask

Seed Round funding for accelerated production scale-up, strategic team expansion, and critical network rollout to meet government demand.

**Quantatest is the only company building sovereign, air-gapped, quantum-resistant infrastructure. The market is mandated. The technology is proven. The team is ready. The time is now.**



© 2026 Quantatest Global. All Rights Reserved.

Made with GAMMA

# The Team, The Plan, and The Ask

**Sole Founder, CEO & Chief Architect** — a hardware security specialist based in Las Vegas, Nevada, with direct expertise in sovereign systems design, lattice cryptography, and critical infrastructure threat modeling. Centralized authority enables rapid execution without committee drag.

## 18-Month Milestones

- Scale full node production for initial client deployments
- Expand network rollout to finance, energy, and defense sectors
- Convert provisional patents to utility filings
- Close first enterprise contracts with recurring protocol fees

## Funding Ask

Seeking **Seed Round funding** to execute a full production run, expand the core engineering team, and accelerate network rollout to key critical infrastructure sectors. Capital deployed directly against verified milestones — not burn rate.

## Go-To-Market

Direct sales to CISOs and CTOs in finance, power, and defense — sectors requiring unconditional technical sovereignty. Physical hardware nodes serve as the primary client acquisition and trust-building tool.

**Reality Check:** All patent filings, technology stress tests, and market numbers referenced in this deck are verified and traceable to foundational sources. Quantatest operates with full transparency — every claim is auditable.

> The fundamental question for any investor: **Would you invest in the company solving retroactive global data theft with sovereign hardware?** This is not a feature upgrade. This is the foundational future of security.



© 2026 Quantatest Global. All Rights Reserved.

Made with GAMMA

# Layer 2 Software Licensing: Quantum-Safe Encryption for AI Cloud & Defense Infrastructure

Beyond hardware nodes, Quantatest offers a software licensing layer for Layer 2 network security, designed specifically for AI cloud infrastructures and defense data centers that cannot deploy full sovereign hardware. Key benefits include PQC-native encryption, cloud-agnostic deployment, regulatory compliance (NIST/NSA standards), and zero hardware dependency.

## Software Licensing Model

- Per-node annual license
- API-based PQC encryption service
- Compliance certification and threat intelligence updates

## Target Markets

- AI cloud infrastructure providers
- Defense data centers
- Financial institutions with hybrid infrastructure
- Healthcare systems requiring PQC compliance



© 2026 Quantatest Global. All Rights Reserved.

Made with GAMMA

# The Inevitable Transition.

Legacy encryption is mathematically obsolete. The 'Harvest Now, Decrypt Later' threat is absolute.

- Option 1: Rely on failing OS-level security.
- Option 2: Own the 21-patent bare-metal successor.

**We are at the end of an era. The cryptographic infrastructure built over the last two decades is actively decaying. Every hyperscale AI cluster and every defense network running legacy encryption today is bleeding its future IP to 'Harvest Now, Decrypt Later' threat actors. You cannot patch this with a software update. You have to lock it at the bare metal. Quantatest holds the 21-patent monopoly on exactly how that is done. Today, we are opening our Seed allocation. We are structuring this as an uncapped round, because placing an arbitrary valuation ceiling on the baseline infrastructure of the post-quantum world is a miscalculation. Furthermore, we are not hiding our architecture behind NDAs and gated portals. Our data room is fully public and accessible right now. The math is proven, the patents are locked, and the Layer 2 payload is live. We have nothing to hide because our moat is absolute. You have the opportunity to own the base layer of the next decade of physical security. The choice is yours.**



© 2026 Quantatest Global. All Rights Reserved.

Made with GAMMA