QuantumShield — Post-Quantum Cryptography Migration Platform

One-liner: The automated platform that migrates enterprise cryptographic infrastructure to quantum-safe standards before Q-Day arrives.

Category: Cybersecurity / Enterprise Infrastructure
Date: February 7, 2026
Timing: Morning Drop

The Opportunity

The Q-Day Crisis

Quantum computers capable of breaking current encryption (RSA, ECC, ECDSA) are no longer theoretical—they're arriving. Intelligence agencies estimate Q-Day (the moment quantum computers can crack current encryption) between 2028-2032. The problem? **"Harvest Now, Decrypt Later"** attacks are happening TODAY.

Adversaries are capturing encrypted data with the intention of decrypting it once quantum capabilities mature. Financial records, health data, government secrets, corporate IP—all being stockpiled for future decryption.

The $50 Billion Problem

- **$326 trillion** in global financial assets rely on vulnerable cryptography
- **Every Fortune 500 company** must migrate to post-quantum cryptography (PQC)
- **NIST finalized PQC standards** in 2024, triggering compliance deadlines
- **US Executive Order** mandates federal systems migrate by 2035
- **EU Cyber Resilience Act** requires quantum-safe encryption for critical infrastructure

Yet most organizations have NO IDEA where their cryptographic dependencies are, let alone how to migrate them.

Why Now?

1. **NIST Standards Finalized** — ML-KEM, ML-DSA, SLH-DSA standards are production-ready
2. **Compliance Clocks Ticking** — Federal mandates create hard deadlines
3. **Enterprise Awareness Peaked** — CISOs are budget-allocated but tool-starved
4. **Crypto Agility is Non-Existent** — Most enterprises can't even inventory their crypto
5. **First-Mover Window** — 18-24 months before big players catch up

---

The Solution

QuantumShield: Autonomous Cryptographic Migration

Vision: Make post-quantum migration as automated as cloud security scanning.

Core Platform Capabilities

1. Cryptographic Discovery Engine

- **Automated scanning** across cloud, on-prem, SaaS, and hybrid environments
- **Binary analysis** — finds embedded crypto in compiled applications
- **Network traffic analysis** — identifies encryption in transit

- **Certificate inventory** — maps all PKI dependencies
- **Code scanning** — detects crypto library usage in repositories
- **API analysis** — inventories encryption across microservices

Output: Complete Cryptographic Bill of Materials (CBOM)

2. Risk Intelligence Layer

- **Quantum vulnerability scoring** for each cryptographic asset
- **Data sensitivity classification** — prioritize by blast radius
- **Dependency mapping** — understand cascade effects
- **Compliance gap analysis** — NIST, CISA, EU CRA requirements
- **Timeline modeling** — when will each asset become vulnerable?

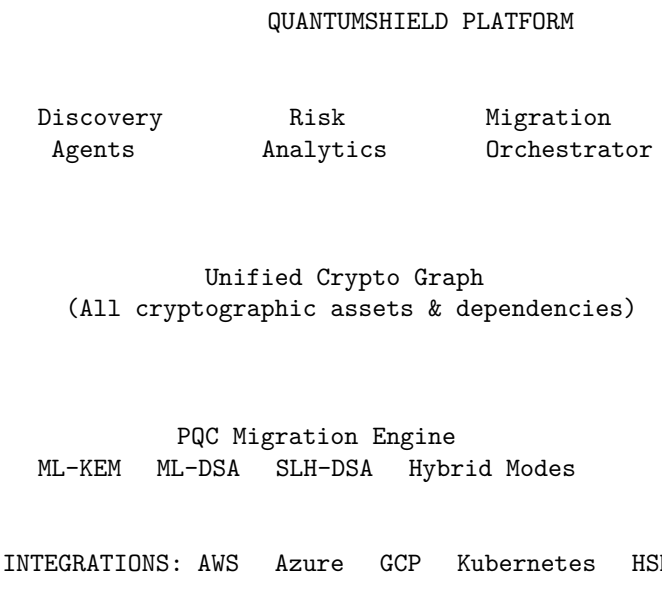
3. Migration Orchestration

- **Automated migration paths** for common scenarios
- **Hybrid encryption deployment** — run classical + PQC in parallel
- **Zero-downtime migration playbooks**
- **Rollback capabilities** — fail-safe migration
- **Certificate lifecycle management** — quantum-safe PKI
- **Key rotation automation** — continuous crypto hygiene

4. Continuous Monitoring

- **Crypto drift detection** — alert when new vulnerabilities appear
- **Compliance reporting** — audit-ready documentation
- **Threat intelligence integration** — quantum computing progress tracking
- **Executive dashboards** — board-ready risk visualization

Technical Architecture



Market Analysis

Total Addressable Market (TAM)

Segment	Market Size	Notes
Enterprise Crypto Management	$12B	Existing market, pre-quantum
PQC Migration Services	$25B	New market, 2025-2035
Quantum-Safe Infrastructure	$15B	Hardware, HSMs, certificates
Compliance & Audit	$8B	GRC tools for PQC
Total	**$60B**	By 2030

Serviceable Addressable Market (SAM)

- **Fortune 2000 enterprises** requiring PQC migration
- **Critical infrastructure operators** (finance, healthcare, energy)
- **Government contractors** with federal compliance mandates
- **SaaS platforms** handling sensitive data
- **SAM: $18B** by 2030

Target Customer Profile

Primary: - CISOs at Fortune 1000 companies - Security architects at regulated industries (BFSI, Healthcare) - Government/Defense contractors

Secondary: - Compliance officers at public companies - Platform security teams at major SaaS providers - Security consultancies seeking PQC practice tools

Competitive Landscape

Player	Approach	Weakness
IBM	Heavy consulting, quantum-safe offerings	Expensive, slow, vendor lock-in
DigiCert	PQC certificates	Point solution, no discovery
Entrust	PKI and crypto	Legacy architecture, no automation
Thales	HSMs with PQC	Hardware-centric, not platform
Big 4 Consultants	Manual assessments	No technology, expensive

QuantumShield's Edge: 1. **Automation-first** vs consulting-heavy competitors 2. **Full lifecycle** vs point solutions 3. **Discovery + Migration** integrated 4. **Cloud-native** vs legacy architectures 5. **AI-powered prioritization** vs manual assessments

---

Business Model

Revenue Streams

1. Platform Subscription (Primary)

Tier	Price	Includes
Starter	$50K/year	Discovery, CBOM, basic reporting
Professional	$200K/year	+ Risk scoring, migration planning
Enterprise	$500K+/year	+ Automated migration, dedicated support

Tier	Price	Includes

2. Usage-Based Components

- **Asset-based pricing:** $10-50/cryptographic asset/month
- **Migration automation:** Per-asset migration fees
- **Compliance reports:** Per-audit documentation packages

3. Professional Services

- **Migration implementation:** 20-30% of platform revenue
- **Training & certification:** QuantumShield certification program
- **Custom integrations:** Enterprise API development

Unit Economics

Metric	Target
ACV	$250K average
CAC	$75K (enterprise sales)
LTV	$1.5M (6-year average)
LTV:CAC	20:1
Gross Margin	80%+
Net Revenue Retention	130%+

Financial Projections

Year	ARR	Customers	Team Size
Y1	$2M	10	15
Y2	$12M	50	45
Y3	$45M	150	120
Y4	$120M	350	280
Y5	$300M	700	500

Go-to-Market Strategy

Phase 1: Beachhead (Months 1-12)

Target: Financial Services & Government Contractors

Why: - Highest regulatory pressure - Largest budgets for security - Fastest procurement cycles for compliance tools

Tactics: 1. **Design partners:** 3-5 Fortune 500 banks for co-development 2. **Compliance-led messaging:** Position as compliance necessity, not security upgrade 3. **CISO advisory board:** Build credibility with industry leaders 4. **Federal certifications:** FedRAMP, FIPS 140-3 validation

Phase 2: Expansion (Months 12-24)

Target: Healthcare, Energy, Technology

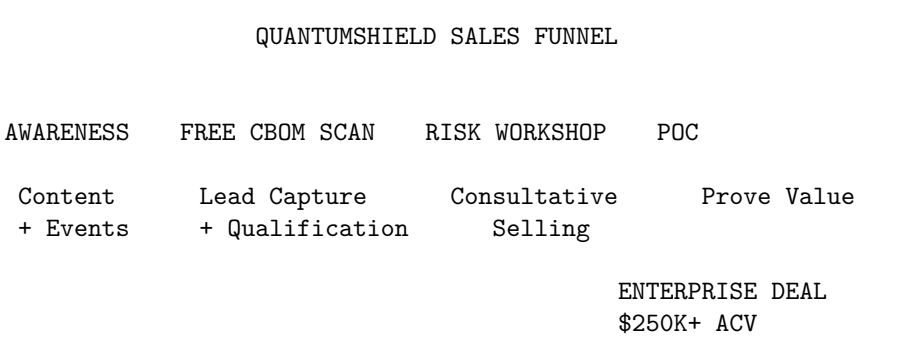
Tactics: 1. **Partner channel:** Big 4 consulting alliances 2. **Industry playbooks:** Vertical-specific migration guides 3. **Conference dominance:** RSA, Black Hat, Gartner Security Summit 4. **Analyst relations:** Gartner MQ, Forrester Wave positioning

Phase 3: Scale (Months 24-36)

Target: Mid-market, International

Tactics: 1. **Self-service tier:** PLG motion for smaller enterprises 2. **MSP program:** Enable security service providers 3. **International expansion:** EU, APAC compliance requirements 4. **M&A:** Acquire niche crypto inventory tools

Sales Motion



Product Roadmap

V1.0 — Foundation (Q2 2026)

- Cryptographic discovery (cloud + on-prem)
- CBOM generation and visualization
- Basic risk scoring
- NIST compliance checklists

V2.0 — Intelligence (Q4 2026)

- AI-powered prioritization
- Dependency graph mapping
- Migration planning tools
- Integration marketplace

V3.0 — Automation (Q2 2027)

- Automated certificate replacement
- Zero-downtime migration orchestration
- Hybrid encryption deployment
- Rollback and testing frameworks

V4.0 — Platform (Q4 2027)

- Partner/MSP white-label
- Industry-specific modules
- Quantum threat intelligence feeds
- Executive reporting suite

Team Requirements

Founding Team (Ideal)

1. **CEO:** Enterprise security sales leader (CISO network, Fortune 500 experience)
2. **CTO:** Cryptography expert (NIST PQC contributor, PhD preferred)
3. **VP Engineering:** Security product builder (detection/response platform experience)
4. **VP Sales:** Enterprise security sales (Palo Alto, CrowdStrike, etc.)

Key Early Hires

- **Cryptography Engineers** (3-5): Deep PQC implementation expertise
- **Security Researchers** (2-3): Vulnerability discovery, threat intelligence
- **Solutions Architects** (2-3): Enterprise customer success
- **Product Manager:** Security product experience

Advisory Board Targets

- Former CISO at major bank (Goldman, JPMorgan)
- NIST PQC standardization contributor
- Federal government security leader
- Enterprise security VC partner

Funding Strategy

Seed Round: $5M

Use of Funds: - Core platform development: 50% - Design partner program: 20% - Team (12-15 people): 25% - Legal/Compliance: 5%

Target Investors: - Cybersecurity-focused VCs (Ballistic, YL Ventures, Ten Eleven) - Strategic angels (former CISOs)

Series A: $25M (Month 18)

Milestone Triggers: - $2M ARR - 10+ enterprise customers - FedRAMP authorization - Working product with automated migration

Use of Funds: - Sales & marketing expansion: 40% - R&D: 35% - International: 15% - Operations: 10%

Series B: $80M (Month 36)

Milestone Triggers: - $40M ARR - Category leadership position - International traction

---

Risks & Mitigations

Risk	Probability	Impact	Mitigation
Q-Day delayed beyond 2035	Medium	High	Focus on compliance mandates (already in effect)
Big tech builds native	Medium	High	Move fast, build integrations, customer lock-in
Migration complexity underestimated	High	Medium	Professional services, partner ecosystem

Risk	Probability	Impact	Mitigation
Talent scarcity (PQC experts)	High	Medium	Early recruiting, training program, acqui-hires
Standards evolution	Medium	Low	Modular architecture, crypto-agile design

---

Why This Wins

Timing is Perfect

- NIST standards finalized
- Government mandates active
- Enterprise budgets allocated
- First-mover window open

Problem is Urgent

- Harvest-now-decrypt-later happening today
- CISOs are panicking but tool-starved
- Compliance deadlines are non-negotiable

Solution is Differentiated

- Only platform combining discovery + migration
- Automation vs consulting competitors
- Cloud-native vs legacy architecture

Market is Massive

- $60B TAM, $18B SAM
- Every enterprise is a customer
- Mandatory, not discretionary spending

Business Model is Strong

- High ACV ($250K+)
- Strong retention (compliance = sticky)
- Platform expansion opportunities

Next Steps

1. **Validate with CISOs:** 10+ conversations to refine problem/solution fit
2. **Assemble founding team:** CTO with cryptography credibility is critical
3. **Design partner:** Secure 1-2 F500 banks for co-development
4. **Seed fundraise:** Target $5M from cybersecurity specialists
5. **Build MVP:** Cryptographic discovery + CBOM generation

Resources

- NIST Post-Quantum Cryptography Standards
- CISA Post-Quantum Cryptography Initiative
- NSA Cybersecurity Advisory on PQC
- EU Cyber Resilience Act

Generated by The Godfather — February 7, 2026

The quantum clock is ticking. Every day of delay is another day of harvested data that will eventually be decrypted. QuantumShield makes the inevitable migration actually achievable.