

Quantum Key Distribution Market Analysis

Disrupting Hardware QKD with Software-Only Solutions

Prepared for



ENTROKEYLABS

Agenda

Executive Summary

Quantum Threat Timeline

Current QKD Market Overview

TAM, SAM and SOM Analysis

Key Players and Competitive Landscape

Hardware QKD Limitations

Cost Analysis by Sector

Trends & Forecast

Market Opportunity Analysis

Strategic Recommendations

Risk Factors and Mitigations

Appendix



Executive Summary



Executive Summary: The Trillion-Dollar Quantum Security Crisis

Market Reality

- Total Market: \$1.85 Trillion TAM
- 10% quantum threat by 2027-2028
- Airforce alone: \$12B/5 years

Entrokey's Solution

- Patented, Software-only = 90% cost savings
- Deploy globally in seconds vs. decades
- No infrastructure requirements
- \$20B addressable opportunity

Available now, while competitors are still in development.

Critical Insights

- Hardware QKD requires new fiber/satellites
- \$60-80K per mile fiber installation
- EU satellites: €280M each
- China already invested \$15.23B

Urgent Action Required

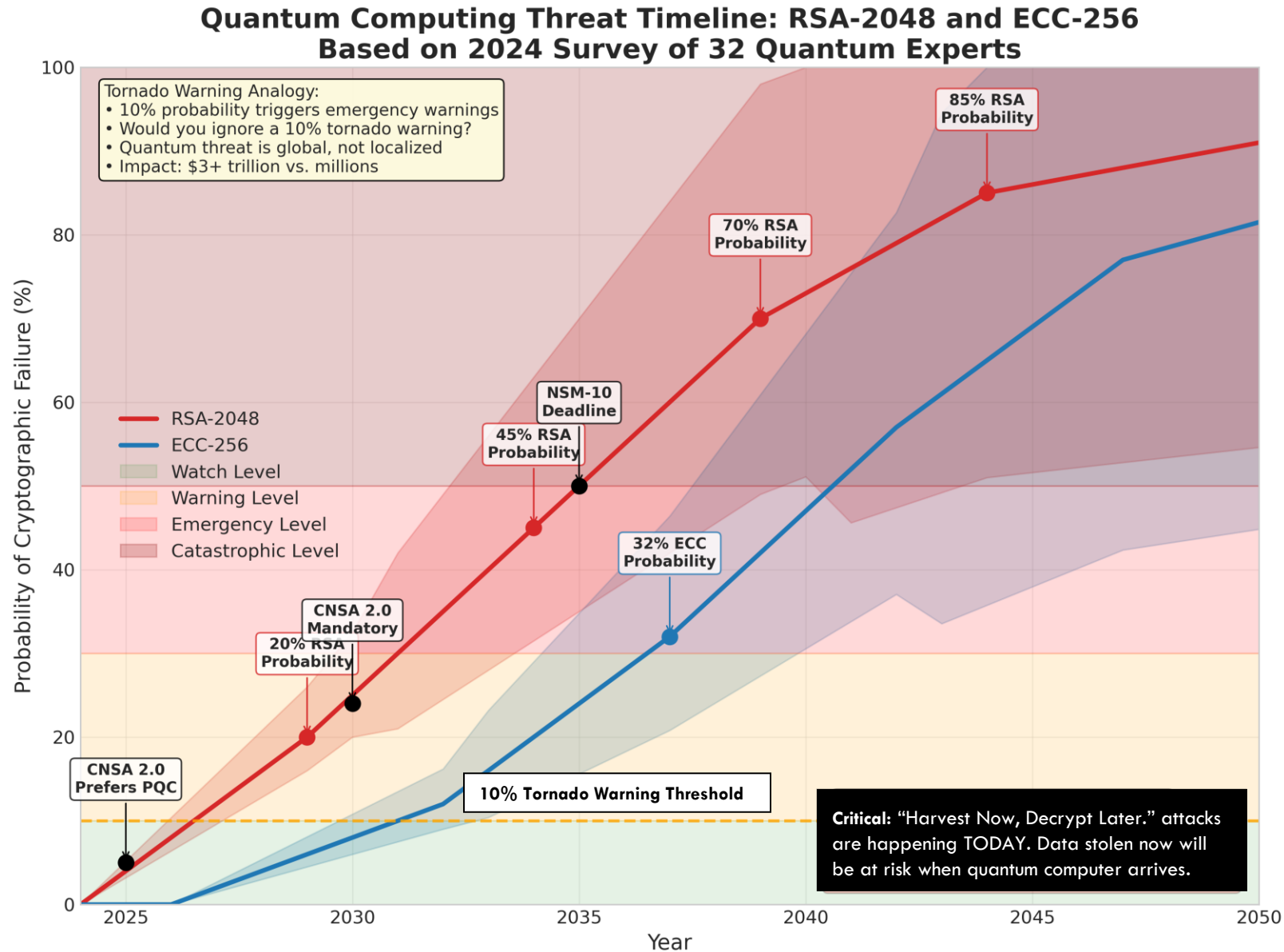
- NSM-10 deadline: 2035
- "Harvest now, decrypt later" happening
- 10% probability = emergency (tornado analogy)
- First-mover advantage critical



Quantum Threat Timeline



The Quantum Computing Threat to Encryption



A Familiar Risk: Natural Disaster vs. Quantum Preparedness

Natural Disaster Preparedness

- **Tornado Warning:** 10% probability triggers emergency alerts
- **Hurricane Katrina:** \$161B damage (regional)
- Preparedness ROI: \$1 invested saves \$4-13
- **Response:** Immediate action, no debate

Question: Would you ignore a 10% tornado warning?

Quantum Threat Preparedness

- **10% Threshold:** Reached by 2027-2028
- **Potential Impact:** \$3+ trillion (global)
- **Response:** Delayed, debated, ignored ?

Critical Difference: Quantum threat is global, not localised.
No safe zones.

Key Message: We do not dismiss a 10% probability of natural disasters like tornadoes, so why disregard an equivalent probability of quantum security threats?



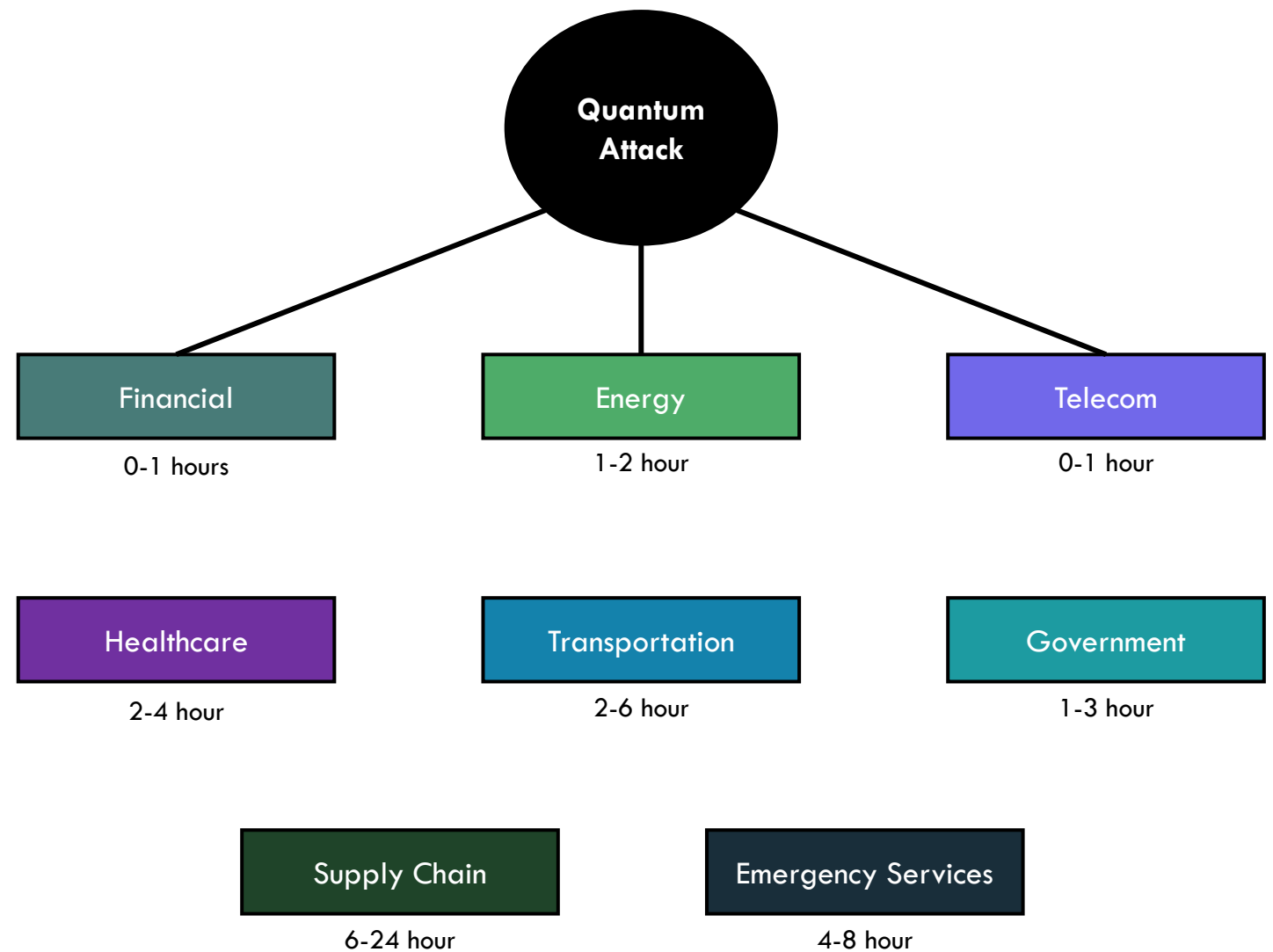
Critical Infrastructure Failure Cascade

Cascade Impact Timeline

- Hour 1: Banking frozen, power grid unstable
- Hour 4: Hospitals on emergency power only
- Hour 8: Transportation gridlock
- Hour 24: Supply chain collapse begins
- Day 3: Complete social breakdown

Economic Impact

- \$500B+ per day globally
- \$3+ trillion if quantum attack sustained
- Permanent data loss from quantum attack
- It will take years to recover from this economic impact



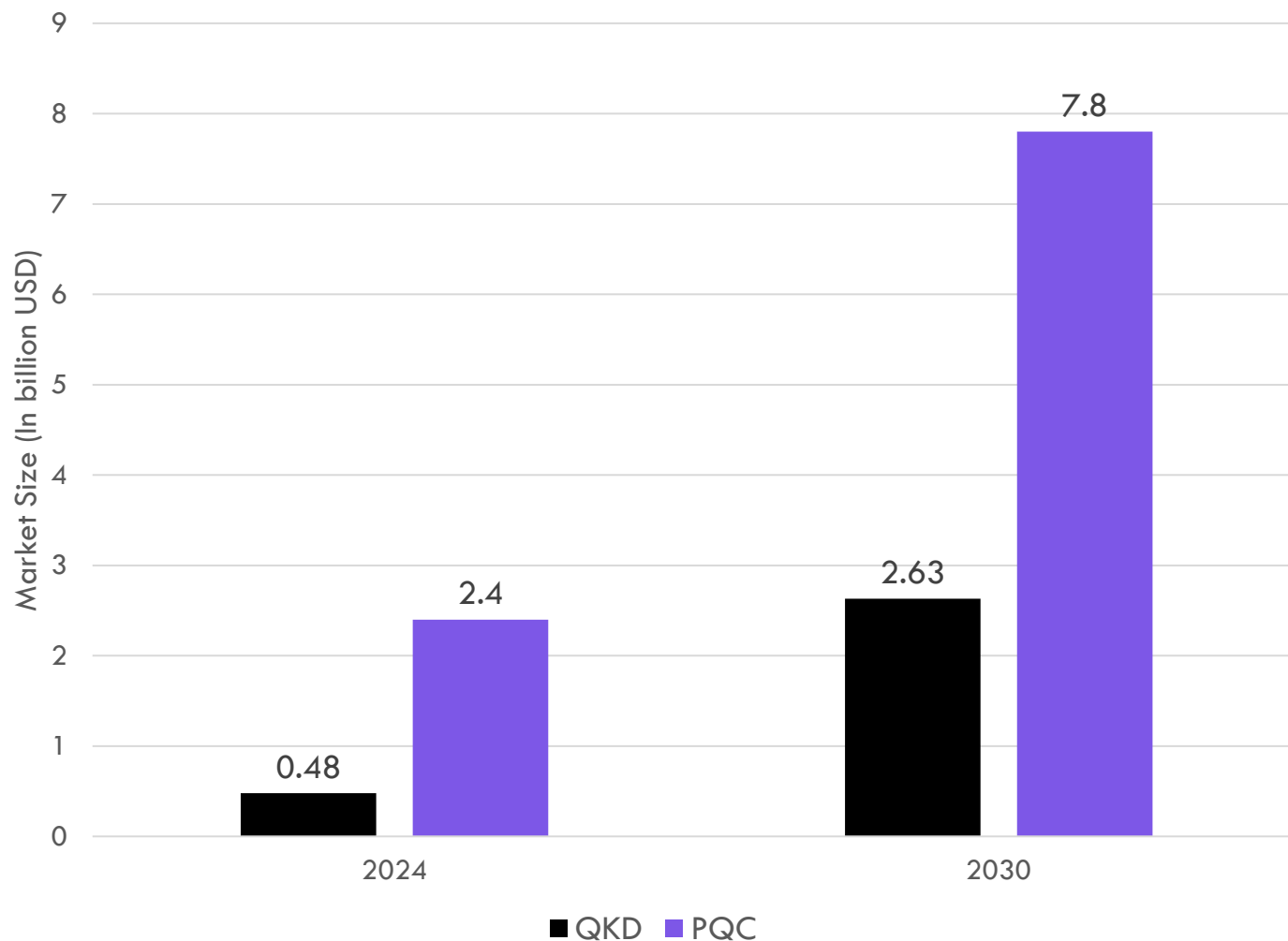
Critical Infrastructure Failure Cascade from Quantum Attack

"No sector is safe when encryption fails"

Current QKD Market Overview



QKD VS PQC Market Size (in Billion USD)



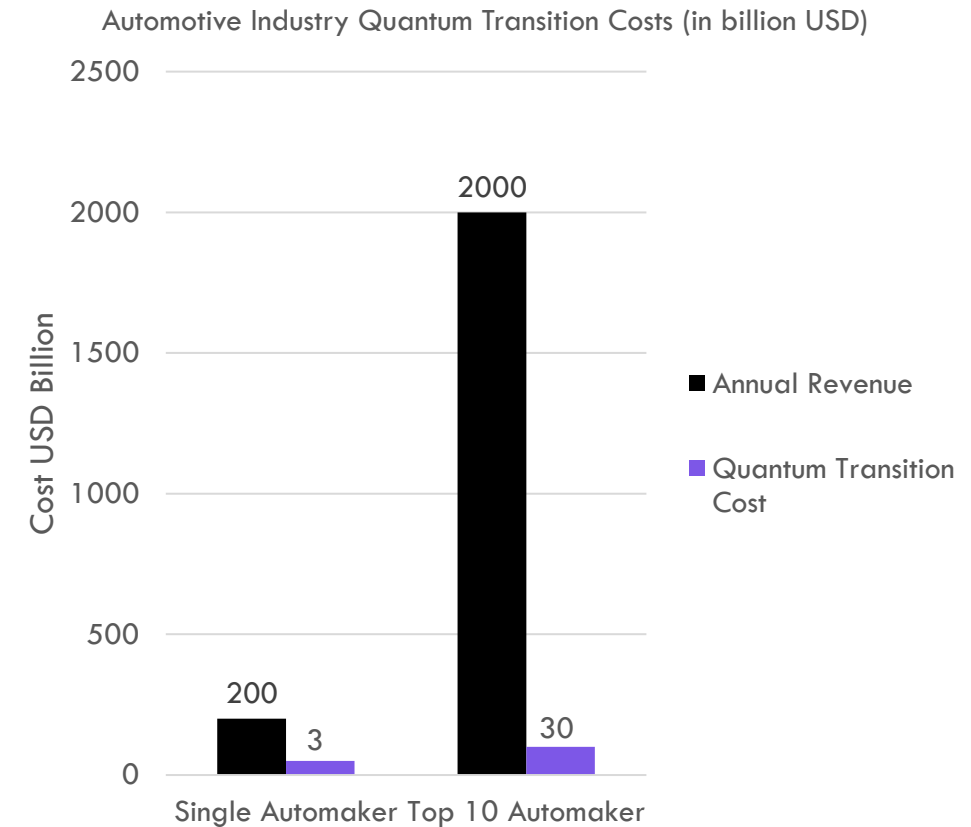
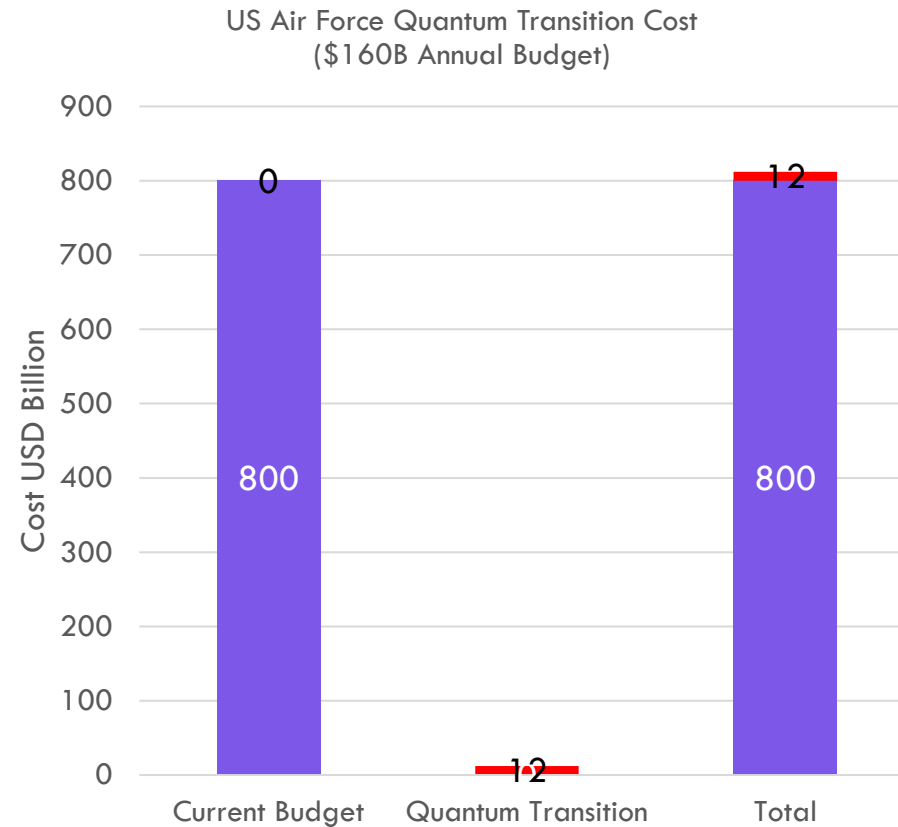
The Trillion Dollar Reality: QKD Market + Infrastructure

- **Growing Market Demand:** The rising QKD market shows increasing interest in quantum-secure communication.
- **Software-Based Advantage:** Software QKD offers a scalable, low-cost alternative to hardware-based systems.
- **Strong Adoption Potential:** It integrates easily with existing systems, making it ideal for wider adoption.



Real-World Transition Costs: Defense & Automotive

Real-World Quantum Transition Costs: Defense and Automotive



Extrapolation to Global Economy:

- If 1.5% of budgets needed for quantum transition

Key Insights

- **Airforce:** 1.5% of the budget over 5 years
- **Automotive:** 1.5% of annual revenue
- Both represents **minimum** requirements



Regional Market Distribution Evolution

North America currently leads the market (37% share in 2024) due to strong government and private investment.

Asia Pacific is the fastest growing region, driven by major national quantum initiatives in China and Japan.

Europe shows high growth potential, spurred by the EU's Quantum Communication Infrastructure (QCI) Project and strong data privacy regulations.

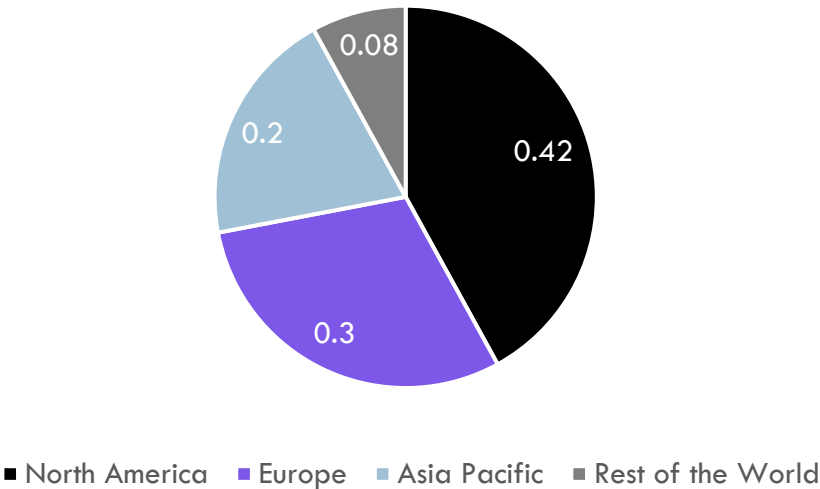
The market is expected to become more globally distributed by 2030 as adoption increases worldwide.



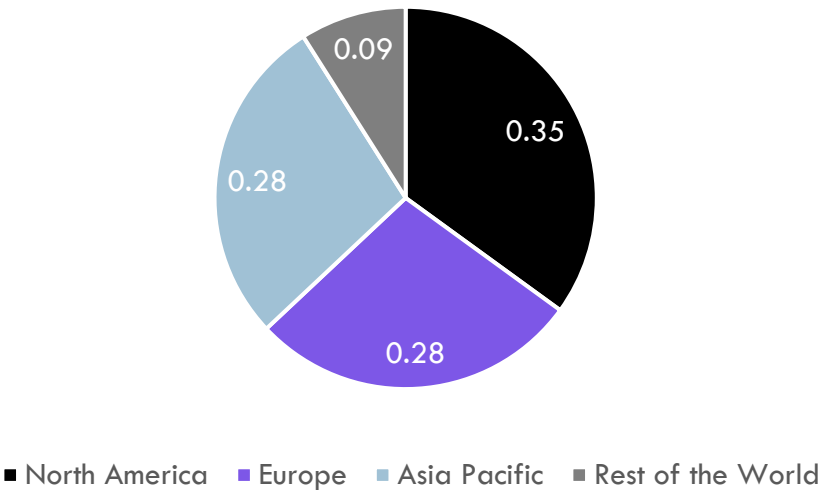
All statistics are sourced. Full citation list available.

QKD Market: Regional Distribution Evolution

2024 Market Distribution (\$480M Total)

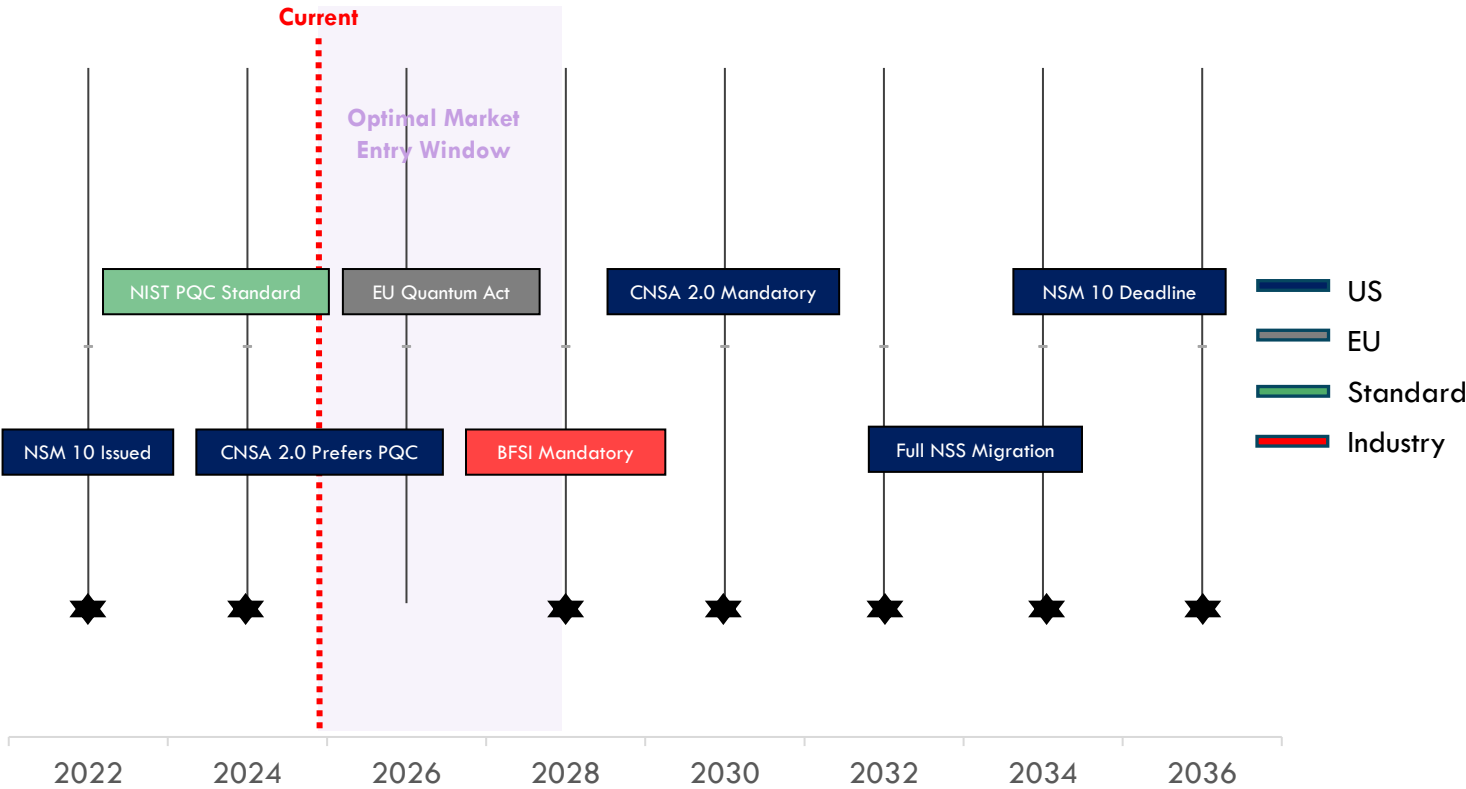


2030 Projected Distribution (\$2.6 Total)



Regulatory Compliance Timeline

Regulatory Compliance Timeline for Quantum Security



Critical Regulatory Deadlines:

- **2024:** NIST PQC Standards published (NOW)
- **2027 - 2028:** 10% quantum threat threshold
- **2030:** CNSA 2.0 becomes mandatory
- **2035:** NSM – 10 DEADLINE-Full migration required

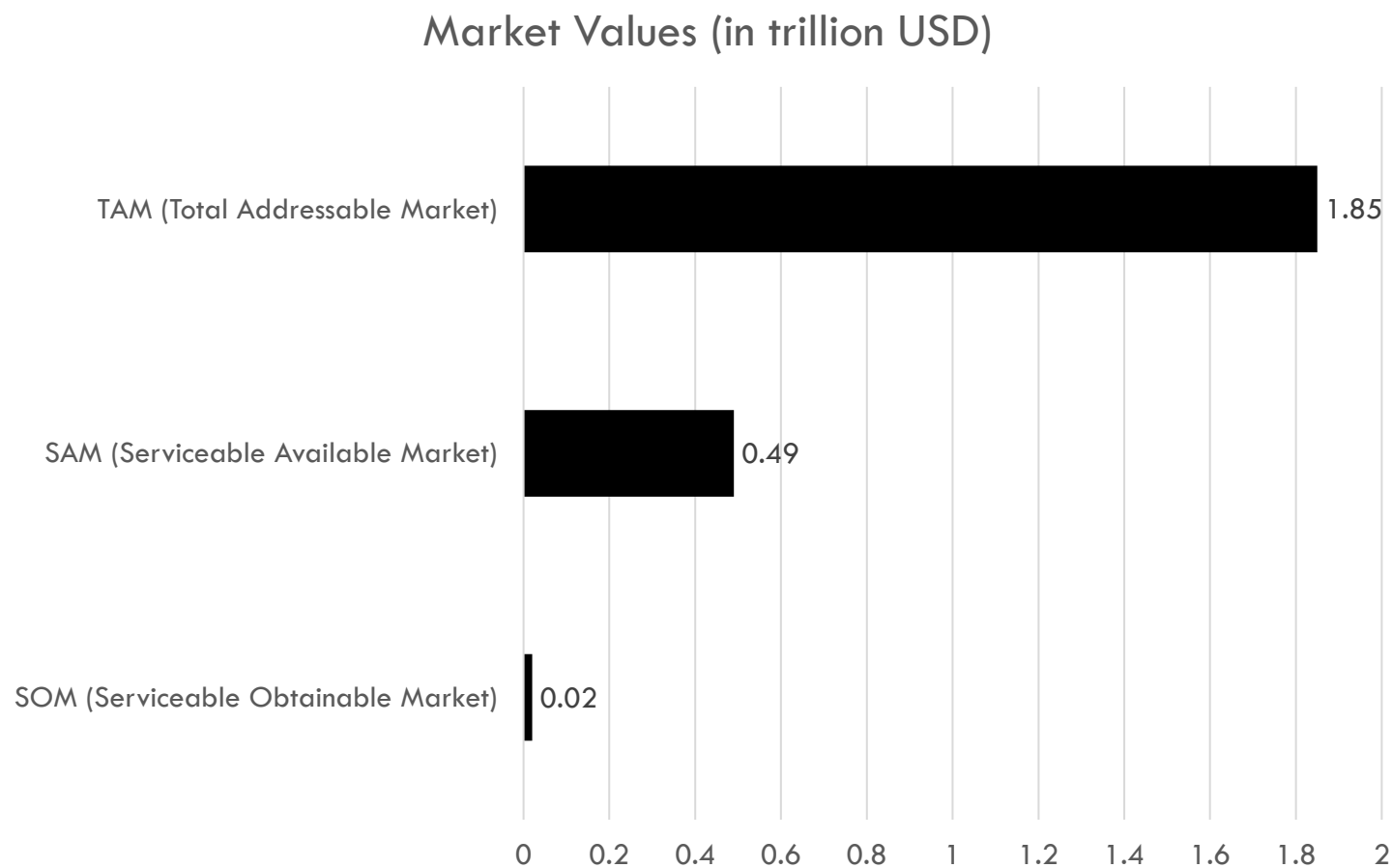
NSM-10 Impact: All U.S. national security systems must be quantum-resistant by 2035. Non-compliance = operational



TAM SAM & SOM Analysis



Market Opportunity: From Trillions to Billions



TAM: \$1.85T

Total Global Quantum Security Need
(Infrastructure + Transition Cost)

SAM: \$490B (\$0.49T)

40% of TAM
(US, EU and Developed Asia)

SOM: \$20B (\$0.02T)

10% capture with software
No infrastructure needed

While hardware QKD requires \$1.37T in Infrastructure, Entrokey's software solution can capture 10% of the market without any infrastructure Investment = \$20 Billion



Market Sizing Data Comparison

QKD Market Size Estimates - Source Comparison

Source	2024 Market Size (USD M)	CAGR (%)	2030 Projection (USD M)	Confidence Score
Grand View Research	446	33.5	2490	9
Markets and Markets	484	32.6	2630	9
Research Nester	2390	21	8000	7
Credence Research	2045	20.25	8941	8
Business Research Insights	2430	19.3	7500	7
Roots Analysis	2000	28.32	30000	6

Note:

- Wide variation in market estimates due to different methodologies
- Conservative estimate used for base case planning
- All sources agree on 20%+ CAGR growth trajectory



Key Players & Competitive Landscape

Current Market Leaders and Entrokey's Position

Quantum Key Distribution: Competitor Summary
Hardware vs Software Solutions Comparison

	ID Quantique	Toshiba	Quintessence Labs	Quantum CTek	MagiQ Tech	Qrypt	Post-Quantum	Entrokey
Founded	2001	2003	2008	2009	1999	2017	2009	2024
Type	Hardware	Hardware	Hardware	Hardware	Hardware	Software-Enabled	Software-Enabled	Software-Only*
Max Distance	100km	120km	80km	100km	140km	Unlimited	Unlimited	Unlimited
Cost/Link	\$100-500K	\$150-400K	\$80-300K	\$100-400K	\$200-600K	\$10-50K	\$5-30K	\$5-20K*
Key Markets	Finance Gov	Telecom Finance	Defence Finance	China Gov Telecom	Gov Research	Enterprise Cloud	Enterprise Gov	All Sectors
Infrastructure	Required	Required	Required	Required	Required	None	None	None

Leaders Quadrant: Dominated by established hardware vendors like ID Quantique and Toshiba.

Visionaries Quadrant: Entrokey is positioned here, with a high completeness of vision due to its software – only approach, but currently lower ability to execute as a new market entrant.

Challengers Quadrant: Includes software – focused companies like Qrypt and Post - Quantum, who are challenging the hardware incumbents.

Entrokey’s strategy is to leverage its unique vision to disrupt the market and move into the Leaders Quadrant.

* **Software-enabled solutions** still require dedicated or specialized hardware, whereas **software-only solutions** operate entirely on existing infrastructure.

* **Entrokey Cost/Link:** It is an early estimate.



Competitive Analysis Matrix

Competitive Analysis Matrix: Hardware QKD vs Software Solutions
Entrokey's Software Advantage Highlighted in Green

	Technology Type	Deployment Model	Distance Limit	Cost per Link	Scalability	Time to Deploy	Geographic Reach	Infrastructure Required
ID Quantique	Hardware QKD	Point to Point	100km	\$100-500K	Limited	Months	Limited	Extensive
Toshiba	Hardware QKD	Point to Point	120km	\$150-400K	Limited	Months	Limited	Extensive
Quintessence Labs	Hardware QKD	Point to Point	80km	\$80-300K	Limited	Years	Limited	Extensive
Quantum CTek	Hardware QKD	Network	100km	\$100-400K	Medium	Years	China Focus	Extensive
MagiQ Tech	Hardware QKD	Point to Point	140km	\$200-600K	Limited	Months	Limited	Extensive
Entrokey	Software	Any Network	Unlimited	\$5-20K	Unlimited	Days	Global	None

All Competitors Required Dedicated Hardware and Infrastructure. Entrokey is the only software-based solution in the market. It's software approach results in reduction cost by 10-100x.

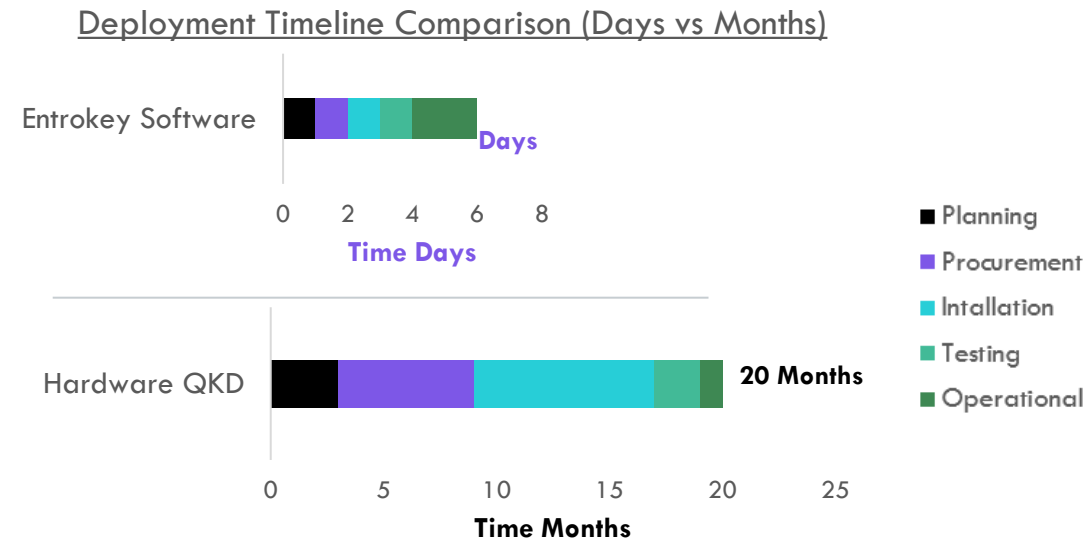
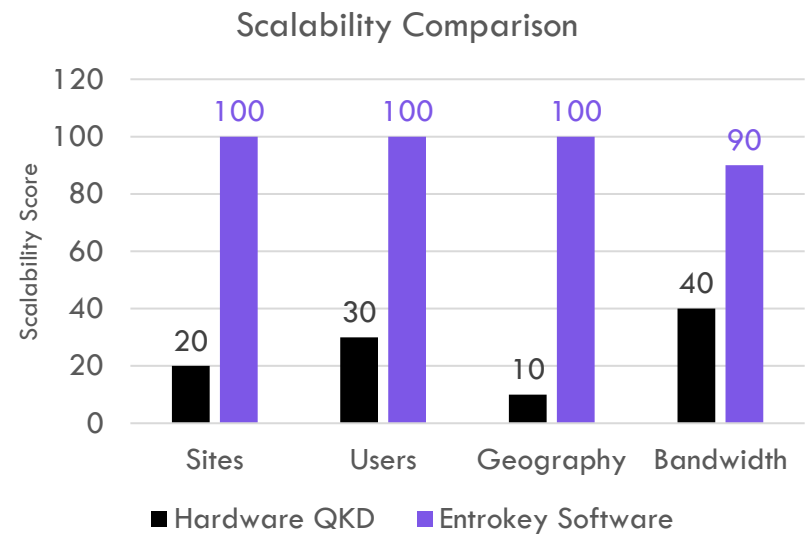
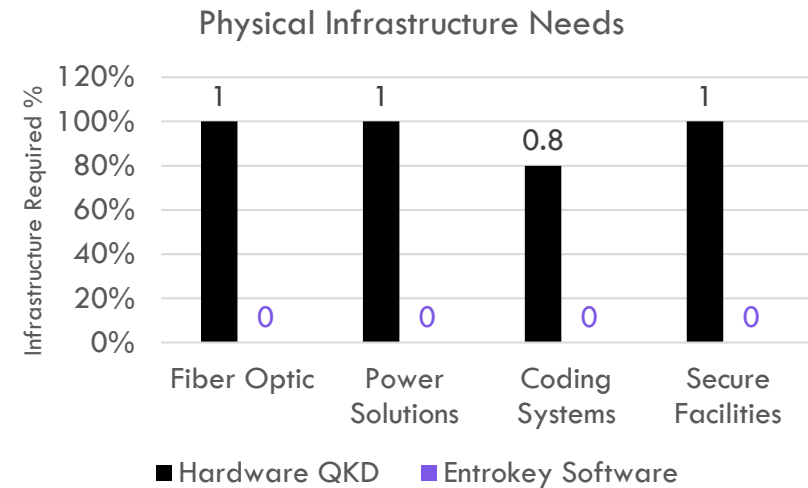
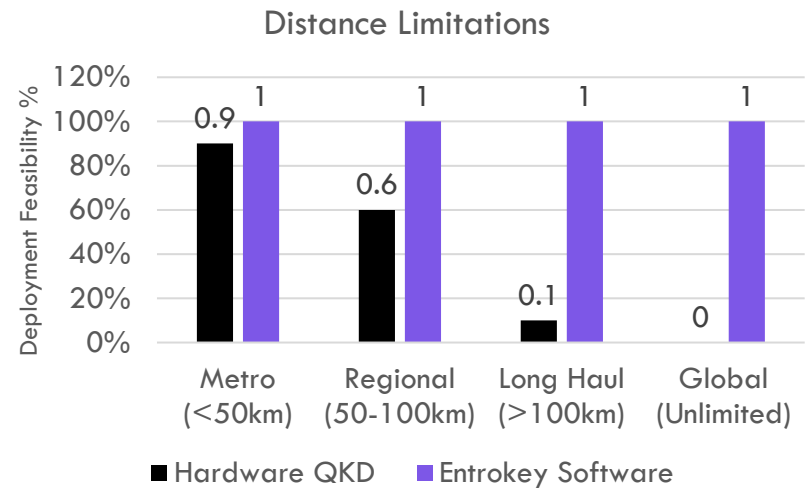


Hardware QKD Limitations



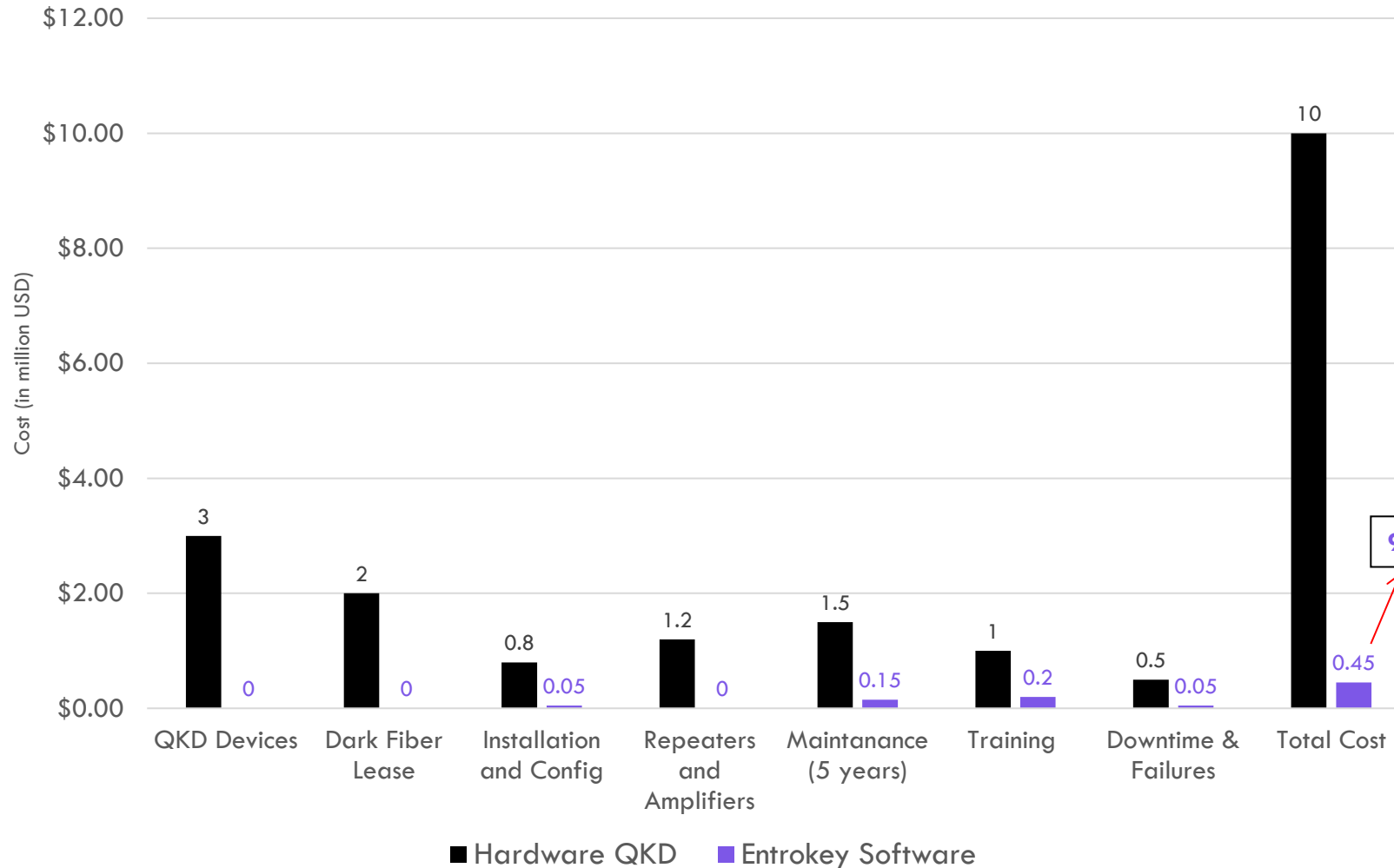
Hardware QKD: The Four Fatal Flaws

Hardware QKD Limitations: Why Software Wins



Hidden Costs of Hardware QKD

Real World Cost Comparison: 10-Site Enterprise Deployment Hidden Costs of Hardware and QKD (in million USD)



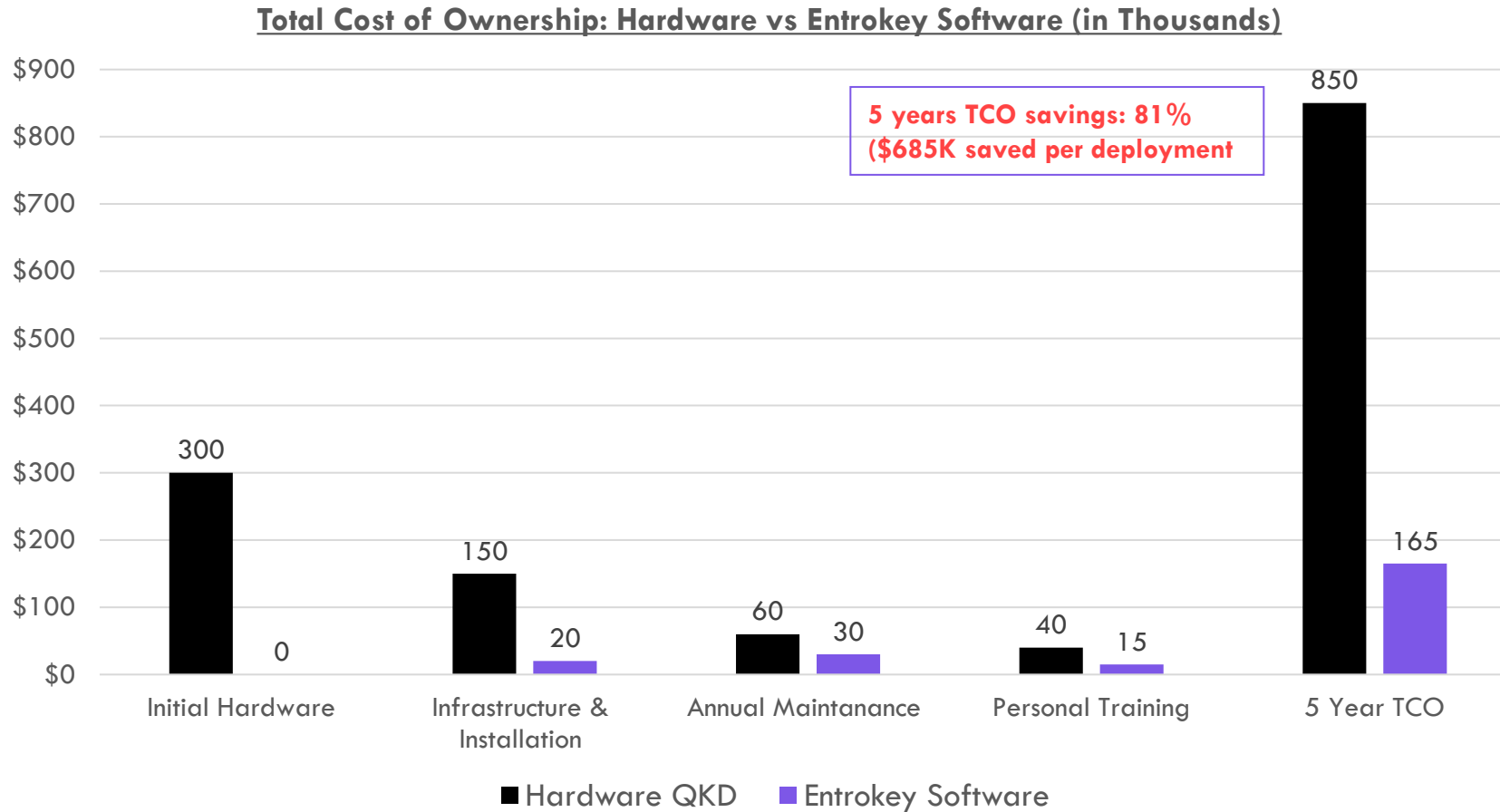
10 Site Enterprise Reality Check:

- Dark fiber lease: \$15 - 20K/month per link (ongoing)
- Quantum repeaters every 50-80km
- 24/7 Monitoring Required
- Single point of Failure = Network Down

90% Cost Reduction



Cost Analysis: Single Link Comparison



Hardware QKD Costs

- Initial hardware: \$300K
- Infrastructure: \$150K
- 5-Year TCO: \$850K

Entrokey Software

- No hardware required
- Minimal infrastructure: \$20K
- 5-Year TCO: \$165K
- 81% cost savings

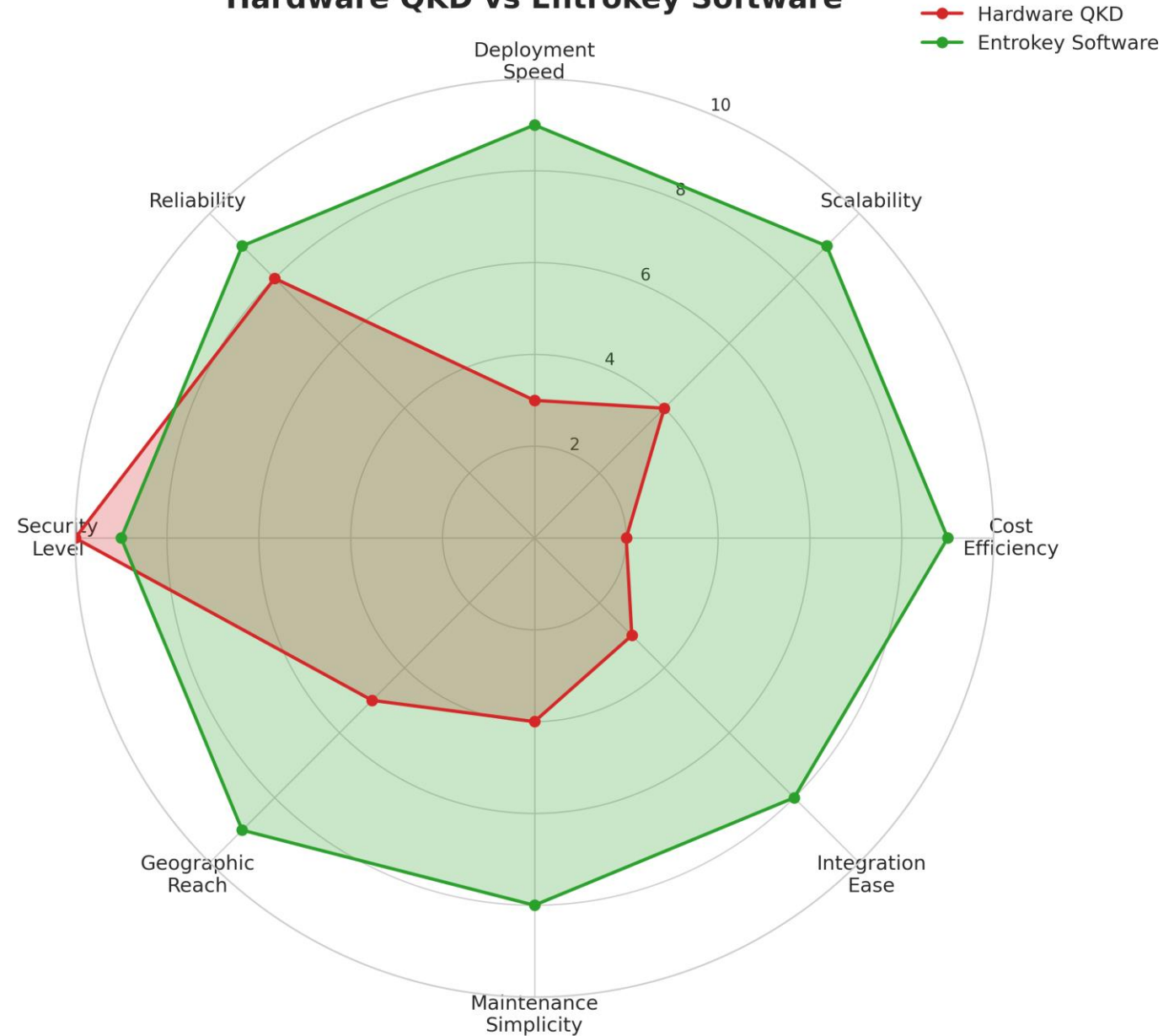


Performance Metrics Comparison

Entrokey Advantages:

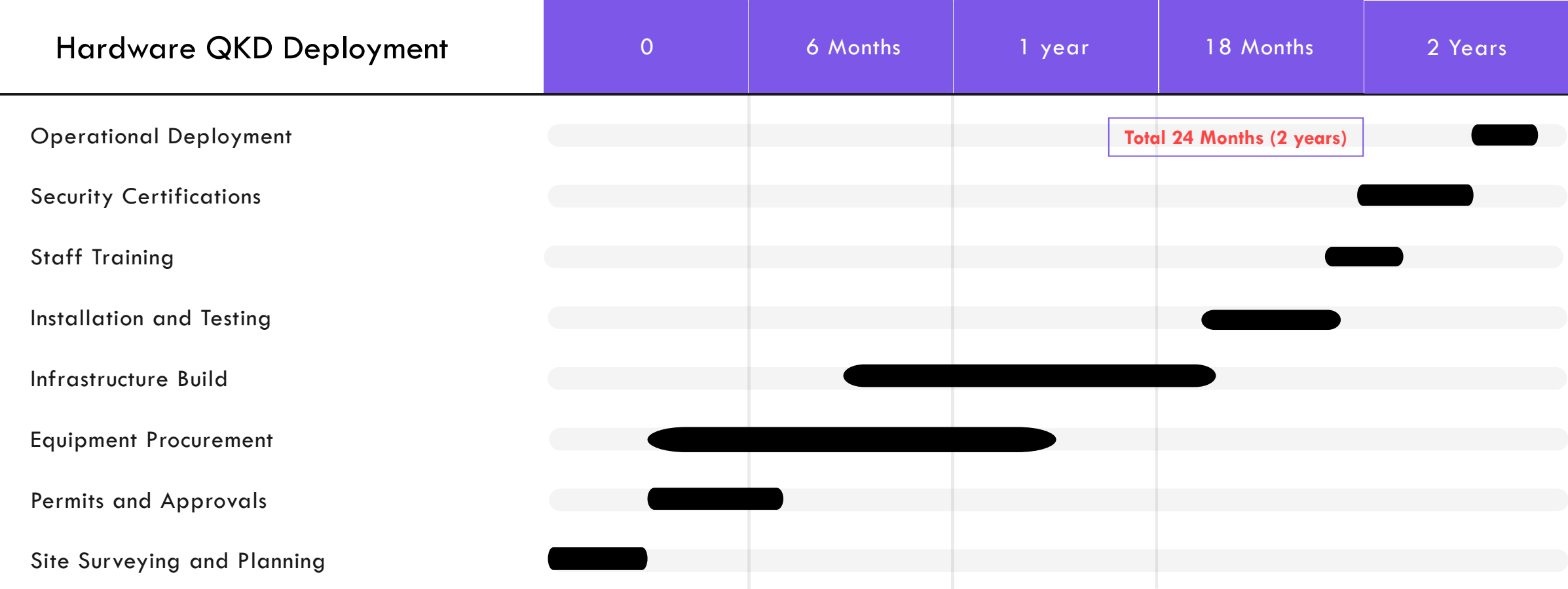
- Superior in 7/8 metrics
- Deployment: 9/10 vs 3/10
- Scalability: 9/10 vs 4/10

Performance Metrics Comparison: Hardware QKD vs Entrokey Software



Deployment Timeline: Decades vs. Days

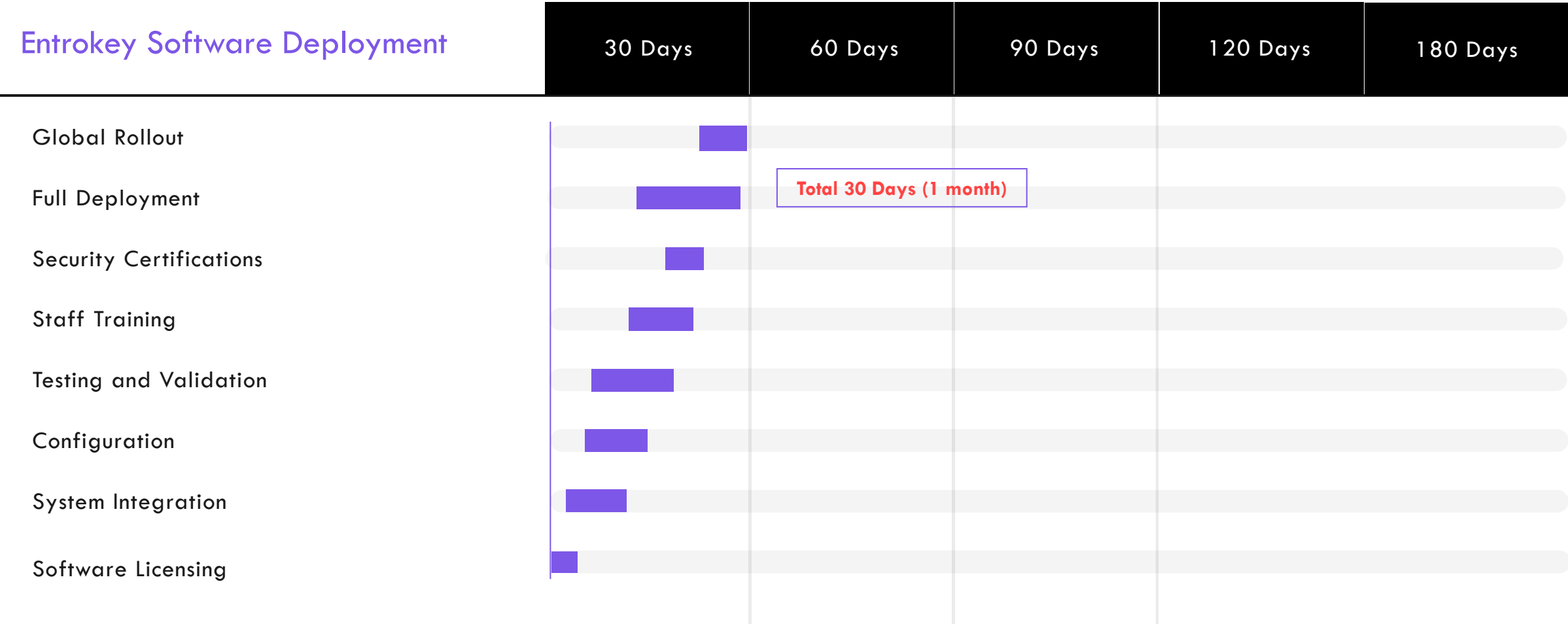
Deployment Timeline Comparison: Hardware QKD vs Software Solution
From Decision to Global Deployment



Hardware QKD takes 2 years for single site deployment and physical constraints limit the scalability.

Deployment Timeline: Decades vs. Days

Deployment Timeline Comparison: Hardware QKD vs Software Solution
From Decision to Global Deployment



- Seamless and efficient integration with existing security architectures, ensuring compatibility and minimal disruption to current operations.
- Entrokey software take 30 days for global deployment with unlimited possibilities of simultaneous scalability.

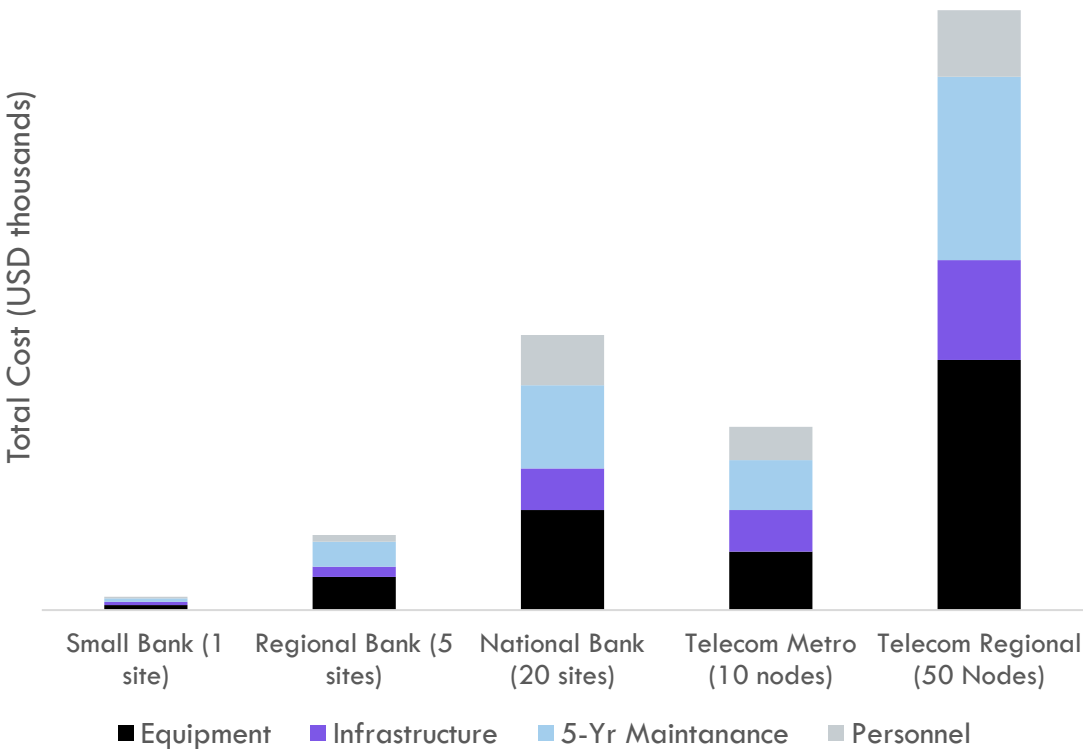
Cost Analysis by Sector



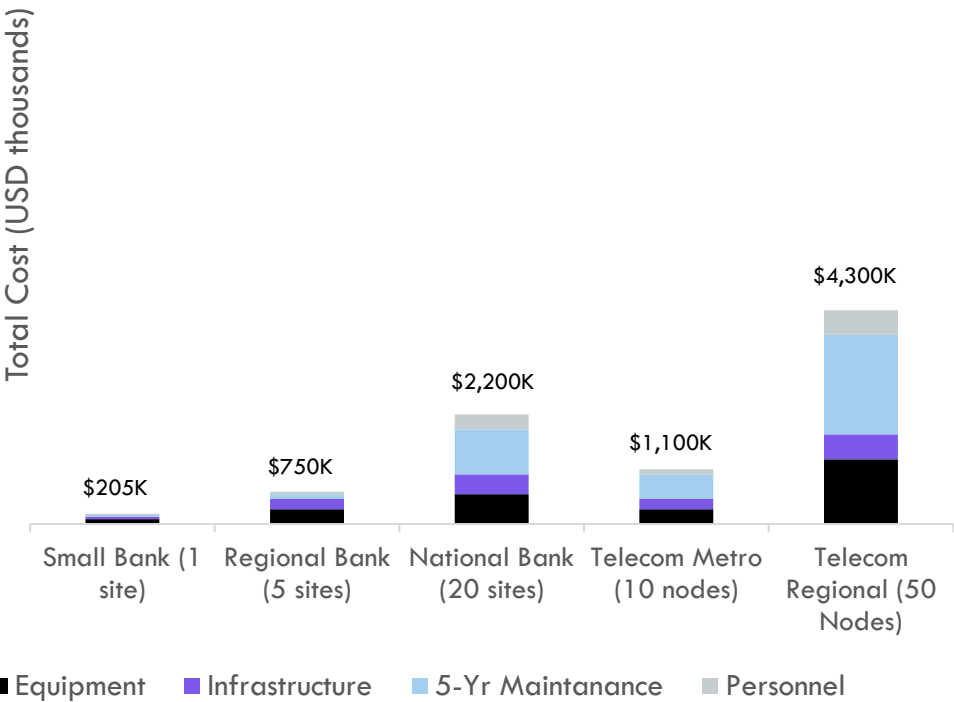
Telecommunications Sector

Total Cost of Ownership: Deployment Scenario Analysis

Hardware QKD: 5 Year TCO



Entrokey Software: 5 Year TCO



Telecom Requirements

Metro networks: 10+ nodes
Regional networks: 50+ nodes

Scalability Challenge

Hardware: Linear scaling
Software: Logarithmic



National Security Sector

Special Considerations

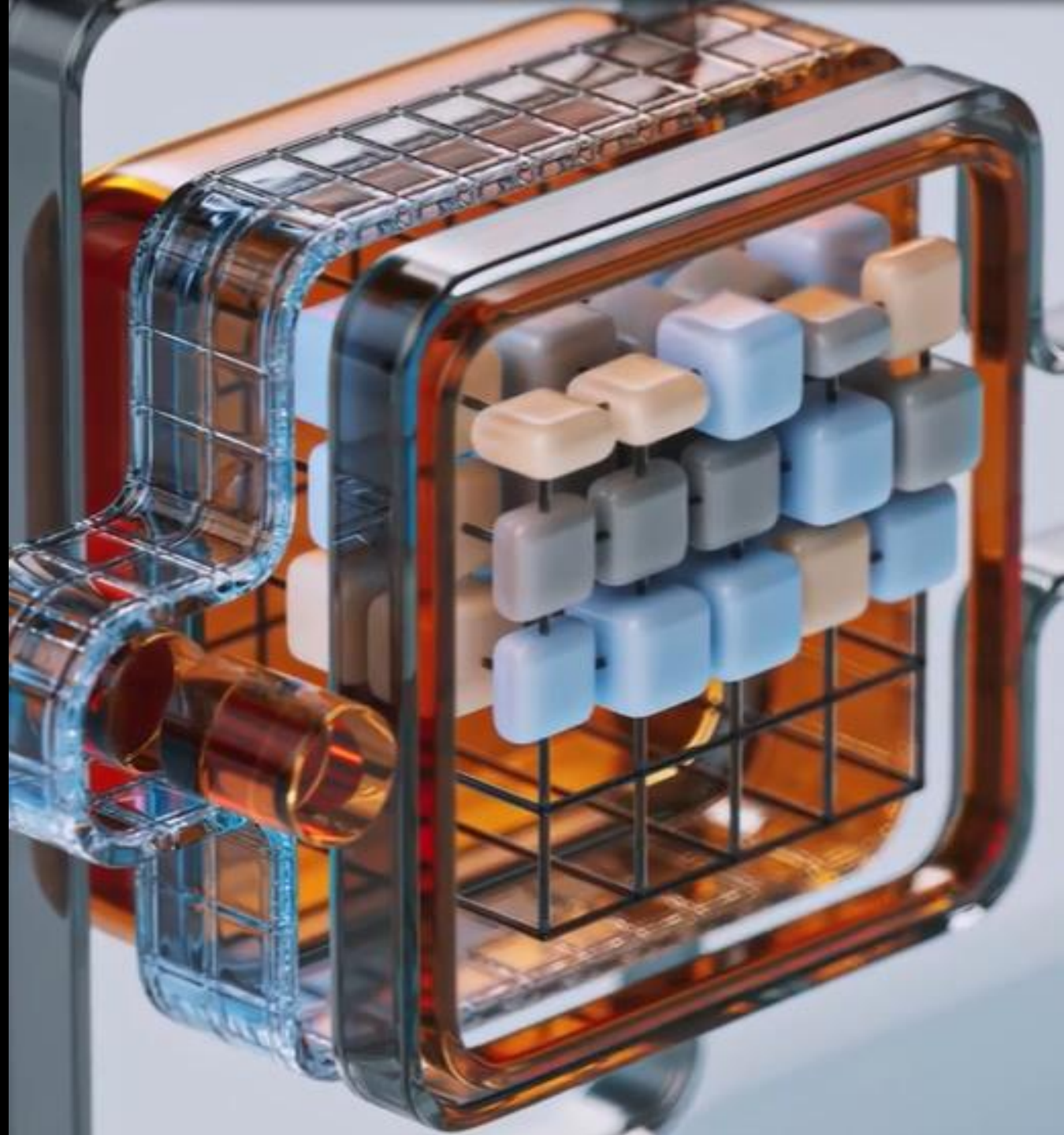
- Air-gapped networks
- Highest security certification
- Redundancy requirements
- Rapid deployment needs

Regulatory Drivers

- NSM -10: Full migration by 2035
- CNSA 2.0: Mandatory 2030 - 2033
- NATO quantum-safe requirements
- Hardware QKD: \$9.5M
- Entrokey: \$1.2M
- [87% savings](#)
- **Faster deployment:** Days vs months



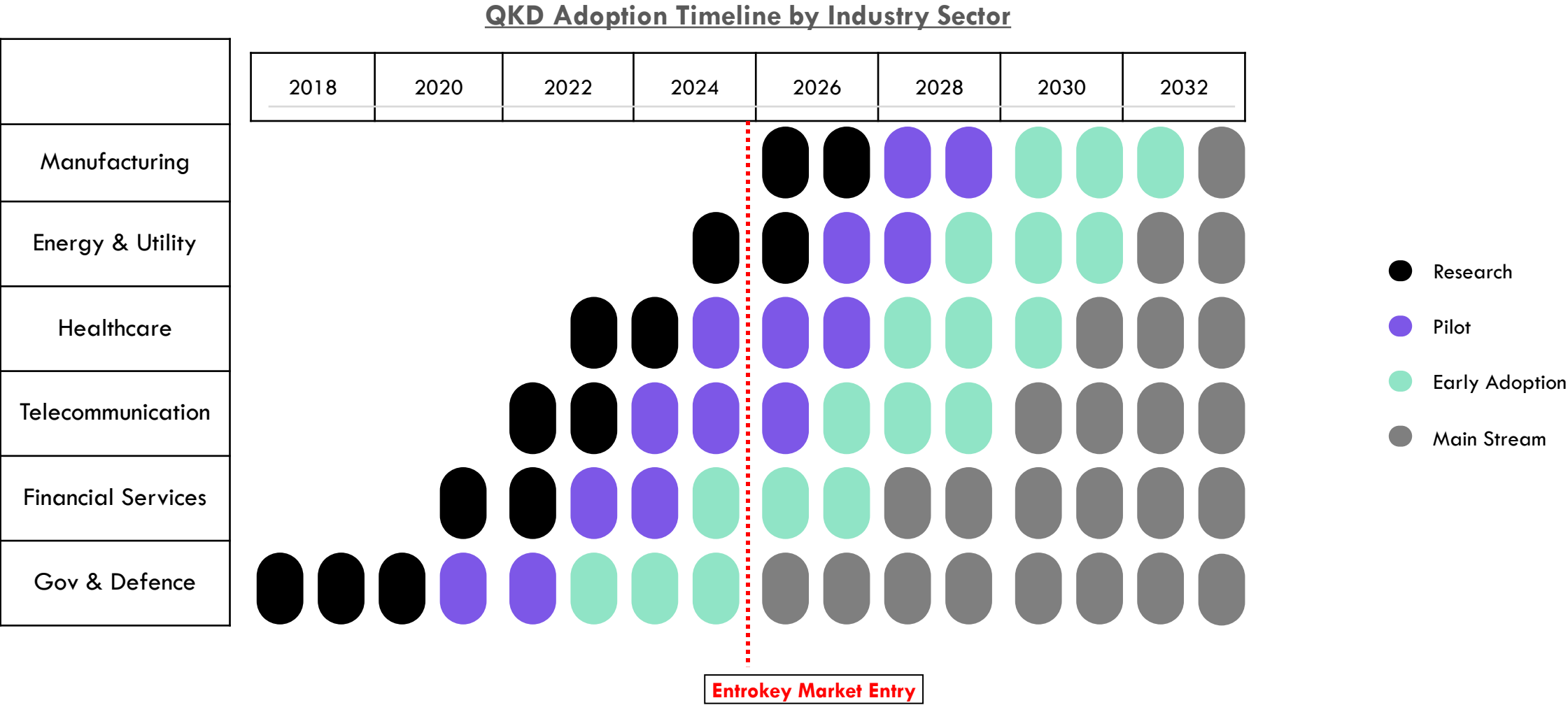
ENTROKEYLABS



Trends and Forecast



Industry Adoption Timeline



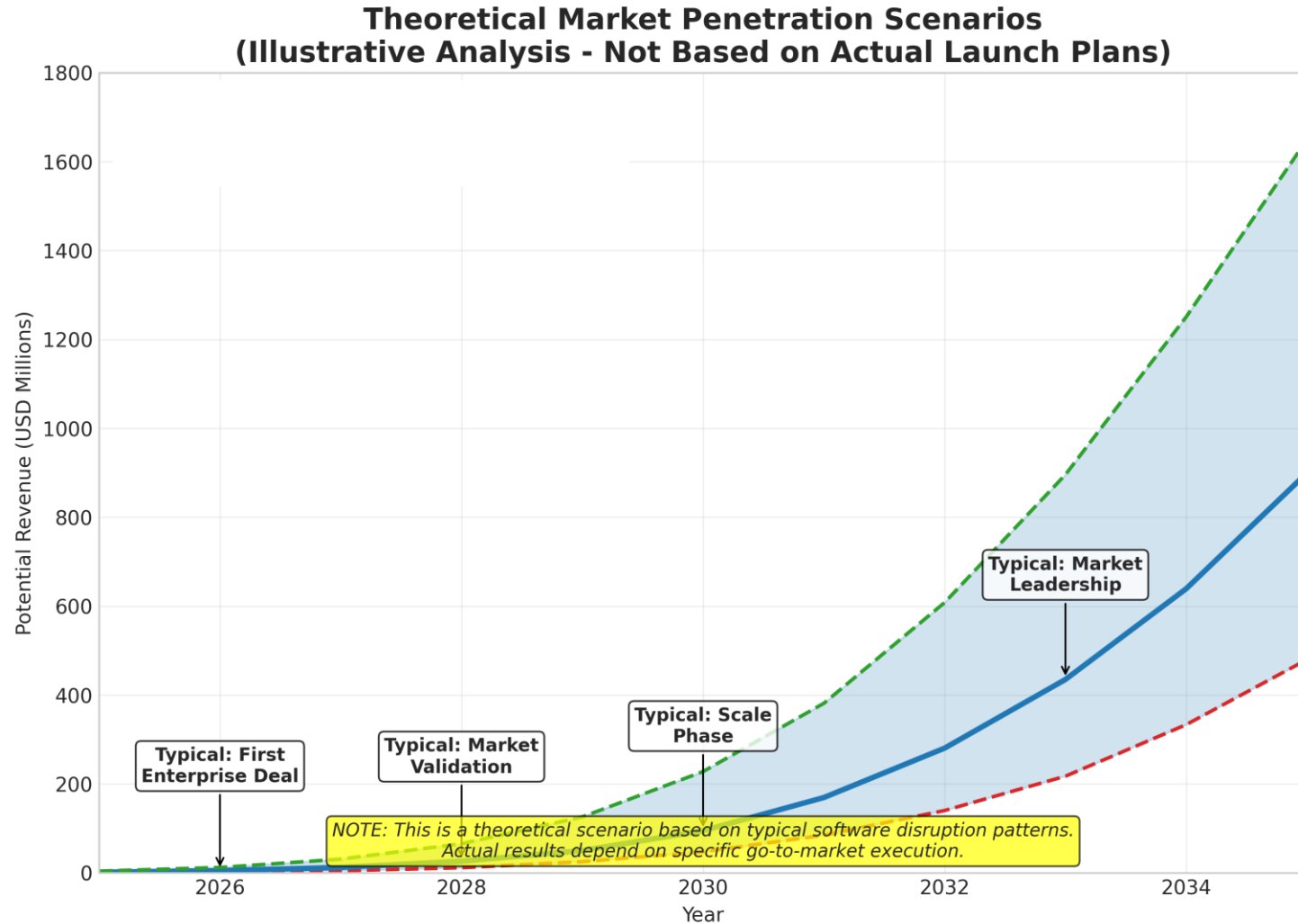
Government/Defense: Already in early adoption phase
Financial Services: Enter in pilot phase
Entrokey market entry: Optimal timing window
All sectors reach mainstream by 2031



Market Opportunity Analysis



Market Penetration Scenarios (Theoretical Analysis)



Illustrative Market Share Scenarios:

- Conservative: \$165M (0.6% share)
- Base case: \$360M (1.2% share)
- Aggressive: \$780M (2.6% share)
- Industry benchmark: 3-5% by 2035

Note: These scenarios are based on typical software disruption patterns in hardware-dominated markets.



Strategic Recommendations



Key Strategic Recommendations



1. Market Positioning

- Position as “QKD democratizer”
- Emphasize software advantages
- Target mid-market enterprises
- Avoid direct hardware competition

2. Go-to-Market Strategy

- Financial services beachhead
- Channel partner program
- Pilot program strategy
- Thought leadership content

3. Product Development

- API-first architecture
- Cloud-native deployment
- Compliance certifications fast-track
- Integration with existing HSMs

4. Funding Considerations

- Deep tech venture capital
- Government grants (quantum initiatives)
- Strategic corporate partners
- Revenue-based growth options



Potential Partnership Opportunities



Technology Partners

- Cloud providers (AWS, Azure, C3)
- HSM vendors (Thales, Entrust)
- Network equipment (Cisco, Juniper)
- System integrators

Strategic Alliances

- Financial institutions
- Government contractors
- Standards bodies (NIST, ETSI)
- Quantum consortiums

Channel Partners

- Cyber security VARs
- Managed security providers
- Telecom operators
- Regional distributors

Investment Partners

- Deep tech VCs
- Corporate venture arms
- Government grants
- Strategic investors



Risk Factors and Mitigation

Key Risk Factors

Technology Risks

- Hardware vendor response
- Security validation challenges
- Integration complexity
- Performance benchmarks

Market Risks

- Slower quantum threat timeline
- Competing standards (PQC)
- Customer education needs
- Long sales cycles

Mitigation Strategies

- Patent portfolio development
- Third-party security audits
- Reference architecture program
- Performance guarantees

Market Mitigation

- Hybrid QKD/PQC offering
- Education program
- Pilot-to-production path
- Channel leverage



Appendix



Methodology

Data Sources

- Grand View Research
- Markets and Markets
- Research Nester
- Credence Research
- Business Research Insights
- Roots Analysis
- ArXiv quantum-ph papers
- Industry interviews
- Government reports (NIST, NSA)
- Company financial filings

Analysis Methods

- Weighted average market sizing
- Monte Carlo growth simulations
- TCO modeling with sensitivity analysis
- Competitive intelligence synthesis

Financial models incorporate projected global GDP growth rates, technology adoption curves, and the accelerating pace of digitization to ensure robust and forward-looking market estimates

Contact Information



ENTROKEYLABS

Entrokey Labs

✉ info@entrokeylabs.com

🌐 www.entrokeylabs.com

Cambridge Frontier Technologies

✉ research@camftl.com

🌐 www.camftl.com

Also see the executive summary.

