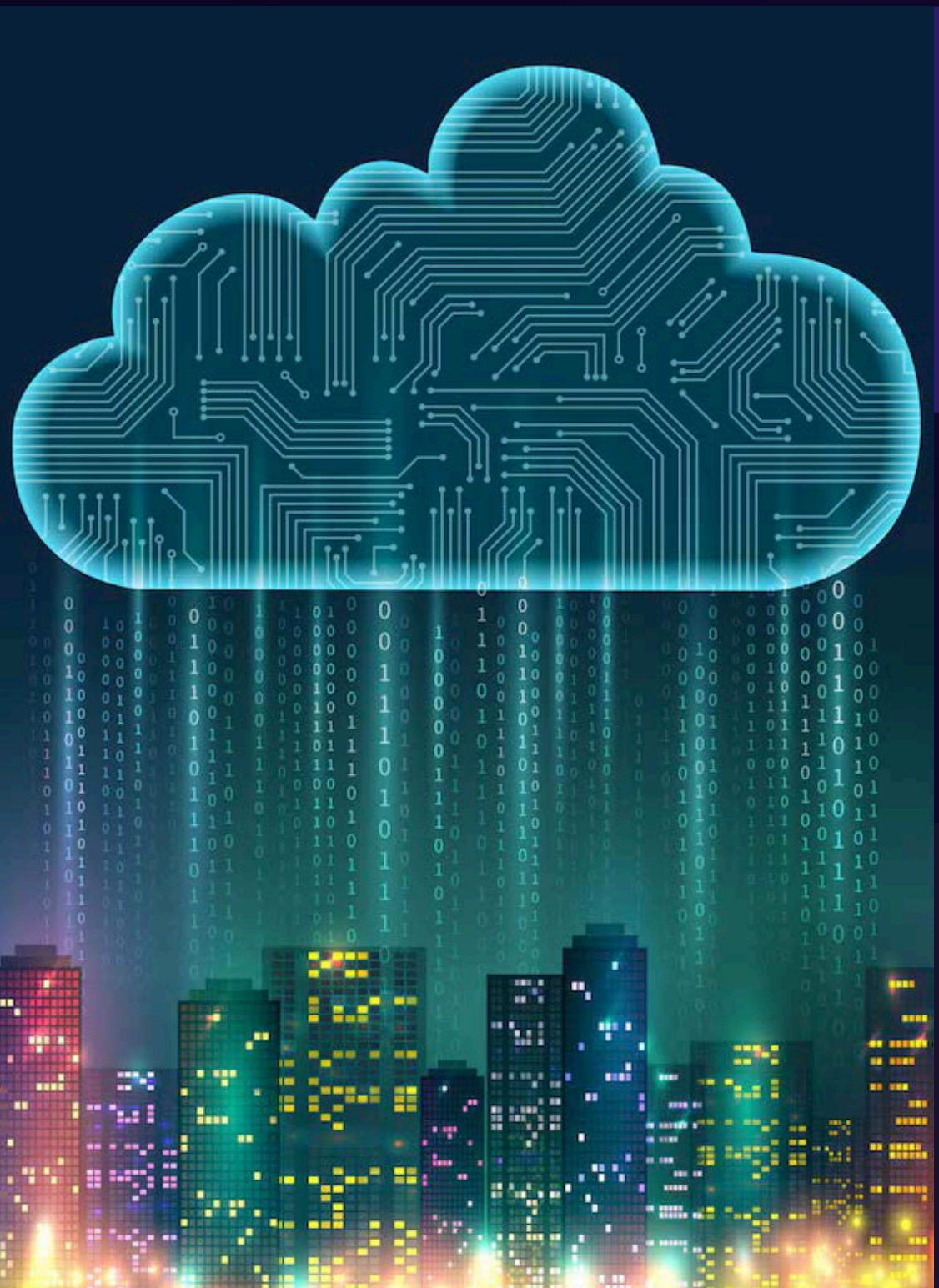
Preparing for the Impact of Quantum Computing on Cloud Security

Protecting digital assets by preparing cloud infrastructure for post-quantum threats.

Pavan Nutalapati

(Technical Leader)

Quantum Computing



It is no longer a future concept — it's becoming real and brings serious challenges to cloud security.

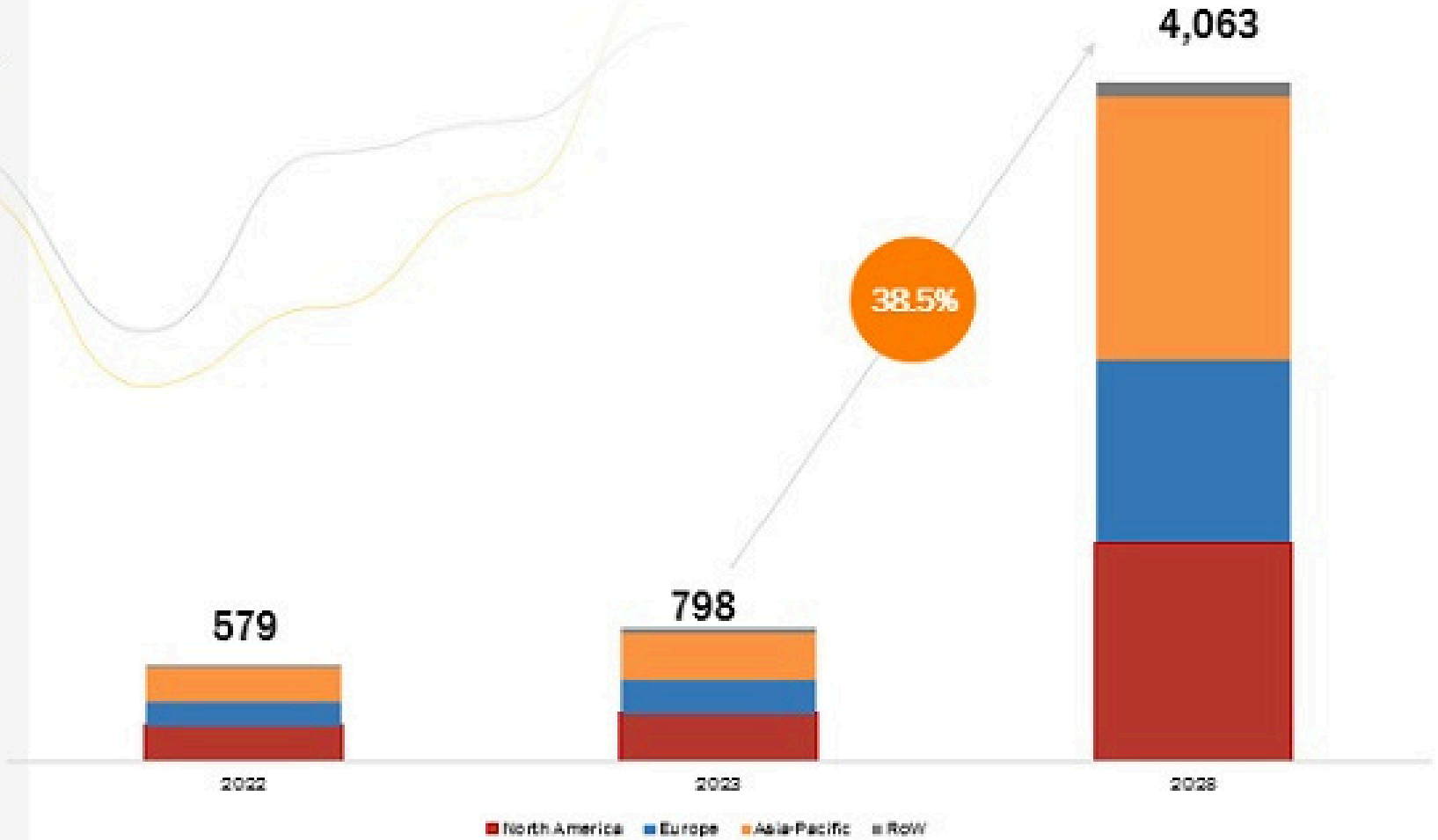
Organizations must act now to prepare!

CLOUD-BASED QUANTUM COMPUTING MARKET GLOBAL FORECAST TO 2028 (USD MILLION)

CAGR OF

38.5%

The cloud-based quantum computing market is expected to be worth USD 4,063 million by 2028, growing at a CAGR of 38.5% during the forecast period.



What is Quantum Computing?

Uses quantum bits (qubits) that can be 0, 1, or both at once.

Enables massive parallel processing, unlike traditional computers.

Far more powerful for solving complex problems, especially in cryptography.

Threatens current encryption through Shor’s algorithm, which breaks codes faster than classical methods.

Cloud Security Today

- 87% of companies use multi-cloud environments.

Current defenses include:

- RSA, ECC (public-key encryption)
- AES (symmetric encryption)
- TLS/SSL for secure communication

Complexity = **Strength, but not quantum - proof.**

How Quantum Computing Threatens Cloud Security

1. Breaks Public-Key Encryption

- RSA & ECC encryption can be cracked by quantum algorithms (e.g., Shor’s algorithm).
- A 2048-bit RSA key could be broken in minutes by a future quantum machine.

2. Weakens Symmetric Encryption

- Grover’s algorithm cuts AES-128’s strength in half.
- AES-256 is recommended for better protection.

How Quantum Computing Threatens Cloud Security (Continued..)

3. Harvest Now, Decrypt Later” Threat

- Hackers steal encrypted data now to decrypt it in the future.
- Sensitive long-term data (e.g., health, finance) is at serious risk.
- 61% of organizations worry about this future quantum threat (DigiCert 2023).

Growing Concerns: The Imminent Reality of the Quantum Computing Threat

61%

have expressed concern their organization is not and will not be prepared to handle security implications that may surface in a post-quantum computing future

---

72%

believe immediate action is required

32%

Only are currently investing in quantum-safe technologies

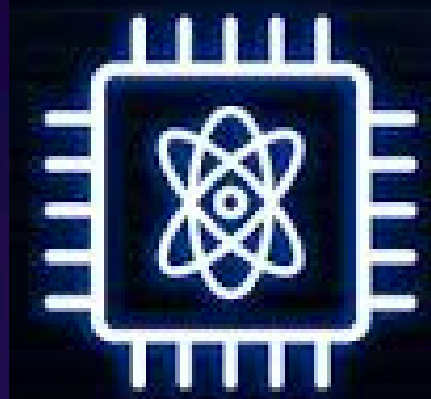
41%

believe their organization must be prepared for a quantum computing era within five years

WAYS TO PREPARE FOR POST-QUANTUM CLOUD SECURITY

- Post-Quantum Cryptography (PQC)
- Quantum Key Distribution (QKD)
- Hybrid Cryptographic Systems
- Cloud Vendor Initiatives
- Cryptographic Inventory & Risk Assessment

How to Prepare for Post-Quantum Cloud Security



1. **Post-Quantum Cryptography (PQC)**

- Develop encryption resistant to both classical and quantum attacks.
- NIST identified 4 standard algorithms (2022):
- CRYSTALS-Kyber (key exchange)
- CRYSTALS-Dilithium, FALCON, SPHINCS+ (digital signatures)

2. Quantum Key Distribution (QKD)

- Uses quantum mechanics for ultra-secure key exchange.
- Detects eavesdropping via quantum state changes.
- High cost & limited range = suited for defense, finance, government sectors.

How to Prepare for Post-Quantum Cloud Security (Continued)..

3. Hybrid Cryptographic Systems

- Combines traditional & quantum-safe encryption.
- Allows backward compatibility + stronger protection.
- Microsoft & Google testing Kyber in TLS connections (e.g., Chrome).

4. Cloud Vendor Initiatives

- Azure: Quantum-safe VPN options
- IBM Cloud: Testing post-quantum algorithms
- AWS: Crypto inventory tools + guidance
- Partner with vendors to plan the transition.

How to Prepare for Post-Quantum Cloud Security (Continued)..

5. Cryptographic Inventory & Risk Assessment

- Identify all encryption types, key lengths & sensitive data locations.
- Prioritize updates for long-term data systems.
- Apply **Zero Trust Architecture** to reduce internal & external risks.

Challenges in Transitioning to Post-Quantum Security

Compatibility Issues
Quantum-safe algorithms often don’t work well with existing legacy systems and devices.

Compatibility Issues
Quantum-safe algorithms often don’t work well with existing legacy systems and devices.

Migration Costs
Upgrading infrastructure demands significant financial and operational investment.

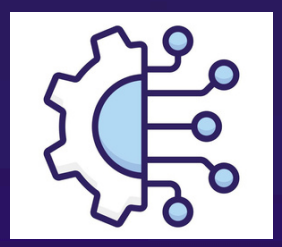
Risk of Inaction
Ignoring quantum threats could be costly.
👉 Average cloud breach = $4.45M (IBM 2023)
👉 Potential losses could rise sharply once quantum attacks become reality..

The Path Forward: Preparing for a Quantum-Ready Cloud

Quantum computing is no longer science fiction—its rapid development demands immediate action from cloud-reliant organizations. To stay ahead, organizations must:

Monitor NIST Standards:
Stay updated with emerging post-quantum cryptographic guidelines.

Collaborate with Cloud Vendors:
Align quantum-readiness plans with trusted providers like AWS, Microsoft, and IBM.



Implement Hybrid Encryption Models:
Combine classical and quantum-safe algorithms for stronger, backward-compatible protection.

Conduct Risk Assessments & Crypto Audits:
Map current encryption use, identify vulnerabilities, and prioritize long-term data protection.

Thank you