FOR IMMEDIATE RELEASE

Qtonic Quantum Corp Launches QScout Surface, Silver, and Gold for Tiered Cyber and Quantum Risk Intelligence

New QScout tiers give executives, CISOs, and boards a staged path from external surface discovery to credentialed validation and internal cryptographic risk intelligence.

Miami, FL, May 21, 2026 — Qtonic Quantum Corp today announced the launch of QScout Surface, QScout Silver, and QScout Gold, a tiered quantum and cyber risk intelligence platform designed to help organizations identify, validate, and prioritize quantum-relevant cryptographic exposure alongside traditional, externally visible, credentialed, and internal security risk.

QScout is built for organizations that need more than scanner output. It combines external discovery, evidence preservation, adversarial validation, and cryptographic posture analysis into one defensible workflow — built to answer a practical executive question:

"What can a capable adversary discover, validate, or exploit across our digital estate, and what should we fix first?"

"Boards and CISOs are being asked to manage two timelines at once," said Mark Stavaski, Vice President of Quantum Sales at Qtonic Quantum Corp. "They have to reduce today's attack surface while also preparing for the cryptographic transition already underway. QScout was built to make that risk visible, evidence-based, and actionable."

QScout Surface: External Risk and Vulnerability Intelligence

QScout Surface is the entry point — unauthenticated, no-credentials external assessment. It maps and evaluates publicly discoverable assets: domains, subdomains, public IPs, DNS, TLS, certificates, mail infrastructure, portals, APIs, authentication surfaces, cloud indicators, public code exposure, and third-party systems.

Surface is designed to identify and validate risks such as:

- Exposed public services and management surfaces
- TLS, certificate, trust-chain, and deprecated-protocol failures
- Static RSA and harvest-now-decrypt-later exposure
- DNS, mail, SPF, DKIM, and DMARC weaknesses, including stale DNS and takeover risk
- Public OAuth, OIDC, and SAML metadata exposure

- Sensitive-path and configuration exposure — .env, .git, Actuator, Swagger, GraphQL, and debug endpoints

Surface suits first-look executive risk discovery, board briefings, M&A diligence, vendor risk review, external attack-surface management, and quantum-readiness triage.

QScout Silver: Credentialed Validation and Application Risk

QScout Silver expands beyond public-only observation by adding controlled, credentialed validation under written authorization — including approved test accounts, synthetic records, application workflows, and access to client-provided artifacts.

Silver determines whether external indicators become confirmed High or Critical findings. It validates:

- Authenticated portal and API exposure, including broken object-level authorization
- Member, customer, provider, and employee workflow risk
- OAuth, OIDC, SAML, session, and public-client behavior
- Repository, dependency, package, and CI/CD exposure
- Secrets, tokens, and key exposure indicators
- Cryptographic library and protocol use

Silver moves teams from “this looks risky” to “this is proven, bounded, and reproducible” — under written authorization and rules of engagement.

QScout Gold: Internal Cryptographic and Quantum Risk Intelligence

QScout Gold provides deeper internal visibility into cryptographic systems, cloud environments, key management, identity infrastructure, architecture artifacts, and post-quantum migration exposure.

Gold is designed for organizations preparing for the post-quantum transition, and for enterprises that need a defensible inventory of where cryptography is used, where sensitive data flows, and where long-lived confidentiality risk exists.

Gold can include review of:

- Cloud, IAM, KMS, HSM, PKI, and certificate inventory
- TLS termination, key ownership, and signing systems
- Internal services, containers, infrastructure-as-code, and CI/CD
- Sensitive data flows, retention windows, and harvest-now-decrypt-later exposure
- Non-agile cryptography and migration blockers
- Post-quantum readiness aligned to NIST-standardized algorithms (ML-KEM, ML-DSA)

Gold helps CISOs and boards see which systems must be modernized first, which keys carry the longest confidentiality horizon, and where quantum migration risk meets real business impact.

Built for Defensible Evidence, Not Noise

QScout uses a quality-controlled, evidence-first model. Findings are separated into confirmed findings, strong indicators, rejected false positives, and not-proven claims — and the platform avoids promoting dangerous-looking output unless the evidence supports it.

Each validated finding can include the affected asset, discovery method, evidence observed, severity rationale, business impact, traditional cyber and quantum relevance, reproduction steps, confidence level, limitations and assumptions, and remediation priority. This gives executives clear risk decisions and technical teams enough proof to reproduce and remediate.

Quantum and Traditional Cyber Risk in One View

QScout is built for the convergence of traditional cyber exposure and quantum-relevant cryptographic risk. A misconfigured portal, weak certificate, or aging TLS configuration may create immediate operational risk. The same systems may also expose long-lived sensitive data to harvest-now-decrypt-later risk.

By combining external attack-path discovery with cryptographic posture analysis, QScout helps organizations prioritize the risks that matter most now — and the risks that will become more urgent as the post-quantum transition accelerates.

> “Quantum risk has moved from the research lab to the boardroom,” said Leandro Corrente, Vice President of Quantum Sales for LATAM at Qtonic Quantum Corp. “The organizations that come through the post-quantum transition well will be the ones that treated it as a governance priority early — and that begins with an honest, evidence-based view of where the exposure actually lives.”

Availability

QScout Surface, QScout Silver, and QScout Gold are available now through Qtonic Quantum Corp. Engagements are conducted under written authorization and rules of engagement appropriate to the selected tier. Organizations can learn more at qtonicquantum.com.

About Qtonic Quantum Corp

Qtonic Quantum Corp is a leading provider of quantum risk and vulnerability intelligence tools and services for organizations preparing for the post-quantum transition. Its platform spans four products: QScout finds risk through continuous, external-first cryptographic visibility; QStrike proves impact through forward-threat validation on real quantum hardware across multiple quantum cloud platforms; QSolve helps fix it with structured post-quantum migration; and Qtonic Quantum Lab independently benchmarks post-quantum cryptography implementations. Together, they give security, risk, and executive leaders the evidence to see where quantum risk becomes business risk — and to act on it.

Media Contact

Jessica Gold
Qtonic Quantum Corp
press@qtonicquantum.com
1-866-4-QTONIC
qtonicquantum.com
