

QuantumGenie Defines Nine-Stage Enterprise Roadmap for Post-Quantum Cryptography

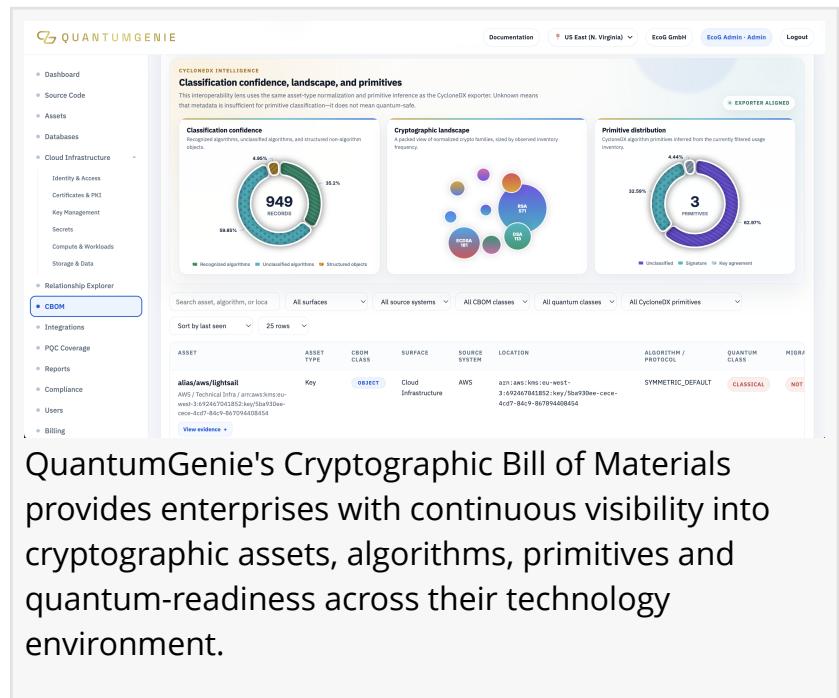
New enterprise lifecycle combines agentless connectors, endpoint telemetry, a 60-field CycloneDX-compatible CBOM, automation, and partner delivery.

NEW YORK, NY, UNITED STATES, October 13, 2026 /EINPresswire.com/ -- [QuantumGenie, Inc.](#), an AI-native platform for post-quantum cryptography discovery, monitoring, attribution and remediation, today announced a nine-stage Enterprise Engagement Lifecycle designed to give organizations a practical, repeatable path from cryptographic visibility to sustained cryptographic governance. The framework gives structure to a field that remains fragmented across digital and manual migration programs.

“

Agentless discovery alone is like sweeping a room while leaving out the corners. Combining endpoint agents with agentless connectors provides the comprehensive signals PQC migration requires.”

*Srijan Dhare, Founder and
CEO, QuantumGenie*



The nine connected stages are: (1) Discovery, to identify cryptographic assets, algorithms, certificates, keys, repositories, services and runtime signals; (2) CBOM preparation, to normalize findings into an evidence-backed Cryptographic Bill of Materials with provenance; (3) Assessment, to evaluate quantum vulnerability, crypto-agility, dependencies, data sensitivity and operational impact; (4) Target architecture, to define the future-state cryptographic architecture, deployment boundaries, integrations and controls; (5) Proof of concept, to validate evidence quality, architecture fit and security controls in a bounded scope; (6) Roadmap, to prioritize remediation waves, owners, milestones, budgets and migration

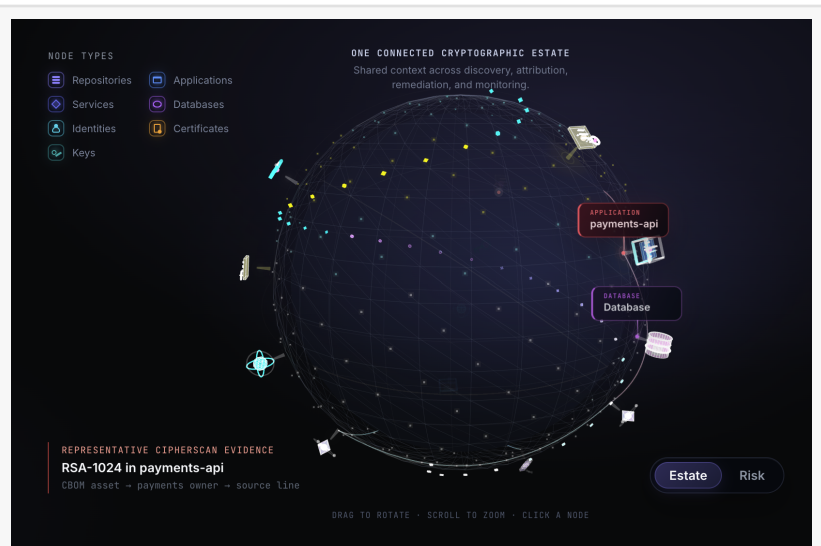
decision gates; (7) Pilot, to deploy to representative systems and validate operating procedures;

(8) Full-scale rollout, to expand approved connectors, endpoint cohorts, remediation workflows and governance; and (9) Continuous monitoring and CBOM maintenance, to refresh evidence, monitor drift and verify remediation.

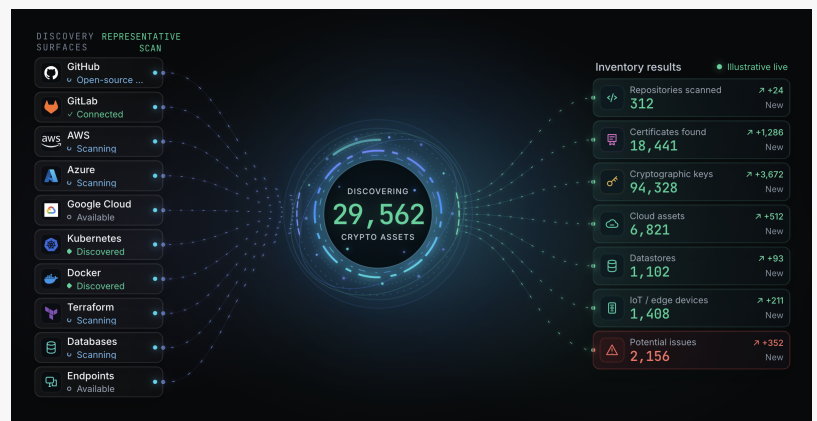
QuantumGenie is designed to support all nine stages in one connected platform. Target architecture and roadmap preparation remain deliberately expert-led because they depend on an organization's risk appetite, operating model, budgets, dependencies and change windows. Across the other seven stages, QuantumGenie can automate up to approximately 80 percent of repeatable discovery, normalization, assessment, validation, rollout telemetry and continuous-monitoring workflows, while preserving human review and approval gates.

Comprehensive cryptographic discovery requires multiple evidence sources. QuantumGenie combines its CipherEdge endpoint telemetry agents with agentless connectors that reuse a customer's existing Microsoft Defender and CrowdStrike Falcon deployments, cloud APIs, source-code repositories, HSM and KMS infrastructure, PKCS #11 interfaces and network SPAN telemetry. CipherEdge provides the deepest local evidence for device and operating-system details, file-signing certificates, local cryptographic libraries, keys, keystores and configuration. Agentless sources broaden coverage without requiring another endpoint deployment: EDR platforms contribute device and software inventory, cloud APIs expose managed keys and service configuration, repositories reveal source-level cryptographic usage, HSM integrations expose managed object metadata, and SPAN traffic provides passive evidence of TLS negotiation and database connections.

All collected evidence is normalized into a canonical model and processed by [CipherScan](#). QuantumGenie's Relationship Explorer connects applications, services, servers, certificates, keys, protocols, libraries, owners and business context so enterprises can see both a cryptographic



QuantumGenie's Security World Model visualizes cryptographic dependencies across repositories, cloud infrastructure, certificates, secrets, identities, and enterprise assets to generate a Cryptographic Bill of Materials (CBOM) and support post-quantum rea



QuantumGenie: AI-Native Cryptographic Discovery, CBOM, Post-Quantum Risk & Remediation

asset and what depends on it. The company's gold standard is an answer at this level: "This netbanking application running on Server 7 uses this TLS certificate containing an RSA-2048 key, issued by AWS and expiring in 69 days, to communicate with this authentication service running on Server 3 over TLS 1.2."

The resulting Cryptographic Bill of Materials is CycloneDX-compatible and can also be exported in CSV, JSON, PDF and XLS formats. QuantumGenie's enterprise CBOM contains 60 fields organized across eight categories: Identity; Ownership and Business Context; Cryptographic Detail; Certificate Detail; Protocol and Library; Discovery and Evidence; Quantum and Risk; and Migration and Governance. This structure turns a flat inventory into an operational migration record with evidence, ownership, dependency, risk, target-state and validation context.

QuantumGenie is applying the same approach to go-to-market execution. Its Partner Program gives resellers, system integrators and managed security service providers distinct commercial and delivery paths through five Prestige Levels: Authorized, Select, Premier, Elite and Strategic. The model connects revenue performance with net-new or repeat customers, certified engineering capacity, production deployments and active managed customers, aligning commercial benefits with demonstrated delivery capability. QuantumGenie is supporting customer and partner engagements in the Middle East and has authorized a Big Four global professional-services organization to market, propose and implement QuantumGenie products in relevant engagements.

About QuantumGenie

QuantumGenie, Inc. is an AI-native post-quantum cryptography platform for cryptographic discovery, CBOM preparation, risk attribution, migration planning, remediation and continuous monitoring. Its product suite includes CipherScan, CipherEdge, CipherNova, the Causal Security Engine, Relationship Explorer and Security World Model. QuantumGenie helps enterprises discover quantum-vulnerable cryptography across code, cloud, databases, networks, HSMs and endpoints; understand operational dependencies; and execute evidence-backed migration toward crypto-agility. Learn more at quantumgenie.ai.

###

Srijan Dhare

QuantumGenie Inc.

+1 339-927-7745

srijan@quantumgenie.ai

Visit us on social media:

[LinkedIn](#)

[YouTube](#)

[Other](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/949318084>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.