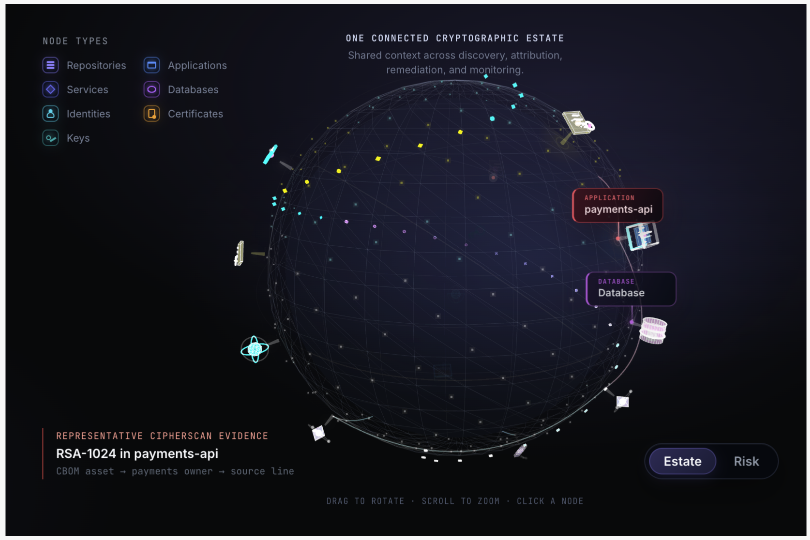
Citibank Selects QuantumGenie for Enterprise Cryptographic Discovery and Post-Quantum Readiness

The partnership uses QuantumGenie's CipherScan platform to build an enterprise Cryptographic Bill of Materials (CBOM) and accelerate crypto agility.



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

NEW YORK, NY, UNITED STATES, July 27, 2026 /EINPresswire.com/ -- What if your emails or whatsapp messages were not encrypted anymore? What if your SSN, passport number, medications, shopping history, crypto wallet address, bank statement, and browser history became public property? Do you believe in conspiracy theories? Well, your wait is coming to an end.

The encryption of today is based on a complex math problem. Funnily, that complex problem is like a kindergarten math for quantum computers, which inherently have the capability to break present-day encryption. Hence the question: Is your data still protected by a kindergarten math problem?

QuantumGenie Inc., an enterprise cybersecurity company specializing in cryptographic discovery, Cryptographic Bill of Materials (CBOM), crypto agility and post-quantum cryptography (PQC), today announced the launch of a formal enterprise cryptographic discovery initiative with Citibank. The engagement will establish visibility into the bank's cryptographic assets and dependencies, creating the foundation for quantum-resistant migration planning and long-term cryptographic governance. QuantumGenie has already completed a 100-device pilot assessment for Citibank (India) and presented an Executive Report in July.

The founder has given a couple of anecdotes that go as follows. Each house has a doorlock. Imagine a master key being built that will be able to open all the doorlocks of the world. This means everyone needs to change their locks. But Harvest Now Decrypt Later goes a step further. Hackers and malicious organisations are already storing encrypted data to decrypt them after

> “Discovery is not a problem. What I am concerned about is what happens after that, and QuantumGenie really stood out and looks enterprise-grade on that front.”
>
> *Vijay Unnikrishnan*

about 2 years. This data spans bank details, personal details (such as SSN, Passport, Address), insurance details, medical records, and most importantly, trade secrets. It has got to be the primary objective of each organisation to perform a so-called cryptographic X-ray of their technical infrastructure, and move on to a well-guided surgery.

Organizations across banking, healthcare, government and critical infrastructure face increasing pressure to inventory cryptographic assets before migrating to NIST-standardized post-quantum cryptography. Attackers are already harvesting encrypted information today in anticipation of future quantum computers capable of breaking traditional public-key cryptography. Without continuous cryptographic discovery and an enterprise Cryptographic Bill of Materials, organizations cannot effectively prioritize migration or manage cryptographic risk.

QuantumGenie’s CipherScan platform continuously discovers cryptographic algorithms, RSA, ECC, digital certificates, cryptographic keys, TLS configurations, cryptographic libraries, protocols and dependencies across endpoints, cloud infrastructure, applications, databases and enterprise environments. The platform generates a continuously maintained Cryptographic Bill of Materials (CBOM) that supports governance, remediation planning, crypto agility and post-quantum migration.

The initiative aligns with the growing adoption of post-quantum cryptography following NIST’s publication of FIPS 203, FIPS 204 and FIPS 205, along with CNSA 2.0 guidance and broader government initiatives encouraging organizations to inventory cryptographic assets and prepare for migration to quantum-resistant standards. In the words of the Enterprise Security Architect of Citibank:

“Discovery is not a problem. What I am concerned about is what happens after that, and QuantumGenie really stood out and looks enterprise-grade on that front.”

“Post-quantum migration begins with visibility,” said Srijan Dhare, Founder of QuantumGenie. “Organizations cannot replace cryptography they cannot see. Our mission is to help enterprises continuously discover cryptographic assets, build an enterprise-grade CBOM and transition to quantum-resistant security with confidence. After discovery comes dependency mapping, and our Security World Model is just that. Do you like to know the Top 500 investors at JP Morgan? Do you like to know the chemical composition of a Pfizer drug? All of these are best kept secrets. Encrypted. But the equation will change in 2 to 3 years. All the encryption of the world could be broken by cryptographically relevant quantum computers, which are not far. AI has expedited their arrival. Every company has secrets. Their own, of their employees, and of their customers. They ought to protect them. The Presidential Executive Order 14412 released on 22nd June already demands all federal enterprises and their vendors to appoint a PQC Migration Lead in July and kickstart the post-quantum readiness activities by September.”

QuantumGenie Inc. is an enterprise cybersecurity company specializing in continuous cryptographic discovery, Cryptographic Bill of Materials (CBOM), crypto agility and post-quantum readiness. Its platform helps organizations identify cryptographic algorithms, certificates, keys, TLS configurations, libraries, protocols and dependencies across enterprise, cloud, endpoint and application environments. The company’s product portfolio includes CipherScan for discovery, CipherEdge for telemetry and CipherNova for AI-assisted remediation.

Srijan Dhare
QuantumGenie Inc.
+1 339-927-7745
email us here
Visit us on social media:
LinkedIn
YouTube
Other
