QuantumGenie Leads Enterprise Post-Quantum Security with Microsoft Marketplace Launch and Google Cloud Validation

QuantumGenie helps enterprises discover cryptographic assets, generate a CBOM, identify quantum-vulnerable dependencies and build a path toward crypto agility.

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

NEW YORK, NY, UNITED STATES, August 11, 2026 /EINPresswire.com/ -- QuantumGenie, the pioneer of post-quantum cryptography that encompasses AI-native discovery, attribution, remediation, and monitoring, today announced its launch on Microsoft Marketplace, arriving alongside the company's Google Cloud Marketplace Solution Validation. Together, these two milestones mark QuantumGenie's emergence as the enterprise standard for post-quantum readiness, giving Azure- and Google Cloud-based organizations a direct path to evaluate its cryptographic discovery and remediation platform inside the ecosystems they already run on.

> “QuantumGenie is the most comprehensive and easiest-to-understand platform we've seen in the Post-Quantum space. Their dashboard and workflow are clean, superior, and remarkably easy to integrate.”
>
> *Ashira Byers*

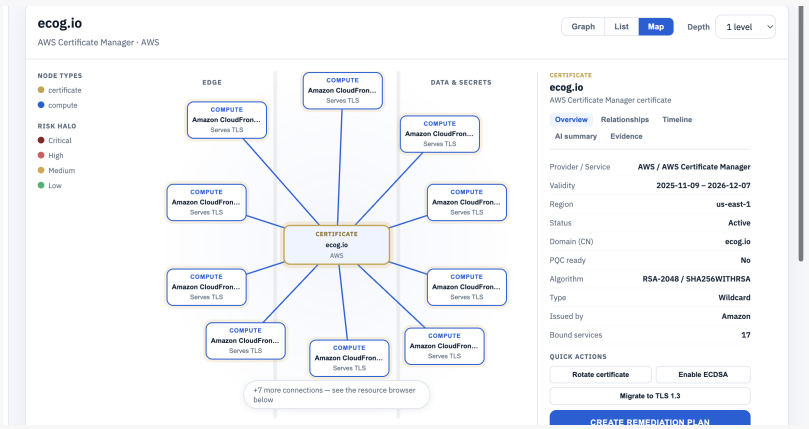
The launch comes as enterprises increasingly prepare for the shift from classical encryption to post-quantum cryptography (PQC). Organizations first need visibility into where cryptography exists across their infrastructure before they can determine what is vulnerable, what needs to migrate, and in what order remediation should occur. No other platform addresses this end-to-end, from a single line of code to a fully remediated enterprise, the way QuantumGenie does.

QuantumGenie is the first platform to take enterprises through the complete post-quantum journey in one connected system, spanning four purpose-built products: CipherScan™ for

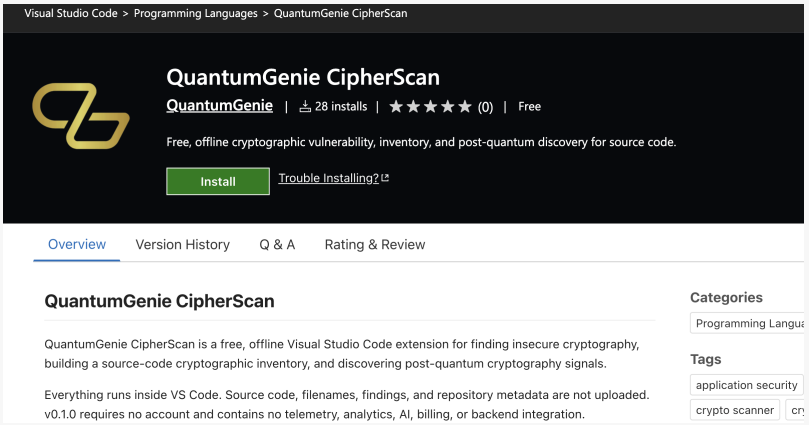
discovery, Causal Security Engine™ for attribution, CipherNova™ for remediation, and CipherEdge™ for continuous, real-time monitoring.

It starts with CipherScan™, which performs one-time or continuous cryptographic discovery through QuantumGenie's numerous integrations across enterprise environments. QuantumGenie supports integration across Microsoft Azure, Amazon Web Services, Google Cloud, GitHub, Bitbucket, GitLab, MongoDB, PostgreSQL, MySQL, Jenkins, Thales, Splunk, CrowdStrike, IBM Cloud, ServiceNow, Datadog, Redis, and other infrastructure and data platforms.

CipherEdge™ is the lightweight endpoint telemetry agent that extends encryption visibility further by capturing network telemetry directly from managed workstations, servers, load balancers, SPAN ports, and IoT devices, completing a full cryptographic map of the enterprise that API-based integrations alone cannot reach.



QuantumGenie also maps certificate dependencies across enterprise infrastructure and provides a path from cryptographic discovery to prioritized remediation and post-quantum migration.



QuantumGenie CipherScan™ on the VS Code Marketplace, providing offline cryptographic vulnerability scanning, inventory, and post-quantum discovery for source code.

Causal Security Engine™ applies this context to attribution and prioritization. It maps the platform's rich cryptographic signals to their dependencies and connected services and assigns each asset a quantum vulnerability risk score, helping security teams move beyond simply identifying a cryptographic weakness toward understanding its root cause, dependencies, potential business impact, and appropriate remediation path.

CipherNova™, QuantumGenie's AI-native remediation engine, closes the loop. It can autonomously patch vulnerable source code and lead certificate migration end-to-end, replacing legacy certificates with hybrid and quantum-resistant certificates. All remediation is performed in accordance with NIST-approved post-quantum algorithms (including ML-KEM, ML-DSA, and SLH-DSA), helping enterprises achieve CNSA 2.0 and FIPS compliance.

At the center of the platform is QuantumGenie's Security World Model™: a continuously updated

representation of an enterprise's cryptographic estate and the relationships among certificates, keys, applications, identities, data, and business services. Rather than treating cryptographic findings as an isolated list of vulnerabilities, the Security World Model™ provides the contextual foundation for understanding how cryptographic assets are connected and what may be affected when a certificate, key, algorithm, library, or protocol changes.

This discovery-to-remediation workflow is central to crypto agility: an organization's ability to understand and change its cryptography without first having to rediscover dependencies during an incident or migration. It is this complete, practical loop (not just another scanner) that positions QuantumGenie as the company defining what post-quantum readiness actually means for enterprises.

QuantumGenie is also available on the Visual Studio Code Marketplace, where CipherScan™ can immediately identify legacy encryption implemented directly in source code. It is supported across more than 10 programming languages, including Python, Java, JavaScript, TypeScript, Go, Rust, C, C++, and C#.

The launch on Microsoft Marketplace gives QuantumGenie an important advantage, demonstrating its compatibility and cryptographic discovery capability within Microsoft Azure deployments. In parallel, its Google Cloud Marketplace Solution Validation confirms the same cryptographic assessment capability for enterprises running on Google Cloud, making QuantumGenie one of the only post-quantum platforms validated across both ecosystems at once.

“Enterprises cannot migrate cryptography they cannot see,” said Srijan Dhare, Co-Founder at QuantumGenie. “It is high time every enterprise appoints a PQC migration lead and starts with at least a one-time cryptographic scan. Frankly, it's surprising there isn't more urgency across the industry yet. What's encouraging is that we're already seeing proactive engagement from the banking and insurance sectors, which makes sense, since both hold enormous volumes of sensitive data that is vulnerable to quantum computers.”

In addition to Microsoft Azure, the platform supports discovery and integration across multi-cloud, source-code, database, endpoint, on-premise and hybrid environments. Last month, the company also began a design partnership with a leading global bank. QuantumGenie therefore approaches post-quantum security as an enterprise lifecycle rather than a one-time assessment:

* Discover the complete cryptographic estate across code, cloud, certificates, keys, infrastructure, and endpoints.
* Generate and continuously maintain a CBOM (Cryptographic Bill of Materials).
* Identify cryptographic vulnerabilities, legacy algorithms, and quantum exposure.
* Map dependencies and determine root cause across cryptographic assets and connected enterprise services.

* Prioritize migration according to vulnerability risk, dependencies, and business context.
* Remediate or guide required changes through automated and guided cryptographic migration workflows.
* Validate the resulting cryptographic posture after remediation and migration.
* Continuously monitor for cryptographic drift, newly introduced vulnerabilities, and emerging exposure.

Cybersecurity in the quantum era requires a system capable of discovering cryptography across heterogeneous enterprise environments, understanding the relationships between those assets, determining what matters most, guiding or executing migration, and then continuously monitoring the resulting cryptographic posture.

That is the category QuantumGenie is building.

CipherScan™ provides discovery and CBOM generation.

Causal Security Engine™ provides attribution, dependency intelligence, and risk prioritization.

CipherNova™ provides remediation and migration.

CipherEdge™ provides continuous cryptographic and network telemetry.

And the Security World Model™ brings those signals together into an evolving representation of the enterprise cryptographic environment.

QuantumGenie has assembled the technology, cryptographic expertise, enterprise integrations, and growing marketplace validation required to pioneer this emerging category. Rather than treating post-quantum readiness as a one-time consulting exercise, the company is building the operational platform through which enterprises can discover, understand, migrate, and continuously manage their cryptography.

The objective is not simply post-quantum readiness.

It is lasting crypto agility.

QuantumGenie, Inc. is an AI-native cybersecurity company focused on cryptographic discovery, attribution, remediation, monitoring, and post-quantum readiness. Schedule a demo at quantumgenie.ai.

Srijan Dhare
QuantumGenie Inc.
+1 339-927-7745
email us here

Visit us on social media:
LinkedIn
YouTube
Other

This press release can be viewed online at: https://www.einpresswire.com/article/932293036

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.