

MARKET NOTE

From Uncertainty to Action: DigiCert Quantum Central and the Race to PQC Readiness

Jennifer Glenn

Philip D. Harris, CISSP, CCSK

EXECUTIVE SNAPSHOT

A new quantum readiness self-service preview provides security teams with a practical first step toward migrating to post-quantum cryptography.

DigiCert, a global leader in intelligent trust serving more than 125,000 organizations, including 90% of the Fortune 500, announced the preview of DigiCert Quantum Central on July 1, 2026, a new solution within the DigiCert ONE portfolio. Quantum Central provides security and IT teams with a practical starting point for post-quantum cryptography (PQC) readiness, enabling cryptographic asset discovery, quantum vulnerability identification, remediation prioritization, and progress tracking via Jira, IT service management (ITSM) tools, and code repository integrations. Offered as a free, self-service preview ahead of general availability in the coming months, Quantum Central addresses a real gap: organizations know PQC migration is coming but lack a practical way to begin and to keep making progress. IDC views this launch as a meaningful step toward operationalizing PQC readiness, though DigiCert must still prove sustained customer value as the solution matures toward general availability.

Key takeaways

- DigiCert Quantum Central gives organizations a concrete, actionable starting point for post-quantum cryptography readiness.
- The free preview lowers adoption barriers, letting teams build cryptographic visibility before committing budget.
- Jira, ITSM tools, and code repository integrations embed PQC remediation directly into existing IT change workflows.
- Quantum Central reflects DigiCert's own PQC migration experience, lending credibility to its guidance and workflow.
- General availability, expected within months, will determine whether preview momentum converts into lasting customer adoption.

Situation overview

DigiCert is a global leader in intelligent trust, protecting the digital world by ensuring the security, privacy, and authenticity of every interaction. Its AI-powered DigiCert ONE platform unifies public key infrastructure, domain name system (DNS), and certificate lifecycle management to secure infrastructure, software, devices, messages, and increasingly, AI content, agents, and models. More than 125,000 organizations, including 90% of the Fortune 500, rely on DigiCert to stop today's threats while preparing for a quantum-safe future. On July 1, 2026, DigiCert extended that portfolio with the preview of DigiCert Quantum Central, a new solution built to help organizations take the first practical steps toward post-quantum cryptography readiness, informed directly by lessons learned from migrating its own infrastructure, products, and services to quantum-safe cryptography.

Solutions and market impact

DigiCert Quantum Central gives security and IT teams a self-service way to discover cryptographic assets, evaluate them against defined readiness policies, and turn violations into prioritized, trackable remediation work. The solution builds inventory from existing DigiCert ONE data and network scans, identifies protocols, cipher suites, algorithms, and key strengths, and integrates with Jira, ITSM tools, and code repositories. Hence, remediation happens inside the workflows teams already use. Reporting dashboards and exportable readiness scores enable organizations to demonstrate their cryptographic posture to auditors, customers, and leadership over time. IDC views this end-to-end workflow, spanning inventory, policy, remediation, and reporting, as a practical answer to a common complaint: guidance on PQC migration is plentiful, but a concrete starting point has been scarce.

For the PQC readiness marketplace, Quantum Central's arrival signals that post-quantum migration is shifting from a compliance talking point to an operational discipline with defined tools and workflows. DigiCert's free preview model lowers the barrier for organizations to begin building cryptographic visibility immediately, ahead of the general availability release expected within the next few months. For customers, particularly those juggling internet-facing transport layer security (TLS) environments, internal public key infrastructure (PKI), software signing, device identity, and vendor dependencies on different migration timelines, Quantum Central offers a way to sequence work realistically rather than treating PQC as a single, undifferentiated project. That sequencing, paired with evidence of progress, can also strengthen customers' positions with regulators, auditors, and enterprise customers demanding proof of quantum readiness.

Benefits of the DigiCert Quantum Central Solution

- Builds complete cryptographic visibility from DigiCert ONE data and network scans across the environment.
- Identifies quantum-vulnerable protocols, cipher suites, algorithms, and key strengths for targeted remediation planning.
- Applies policy rules to flag non-compliant cryptography automatically as inventory changes over time.
- Converts policy violations into prioritized change requests with predefined, context-aware remediation templates.
- Integrates with Jira, ITSM tools, and code repositories to track remediation inside existing IT workflows.

IDC'S POINT OF VIEW

IDC views DigiCert Quantum Central as a showcase for how post-quantum readiness can move from abstract guidance to a concrete, sequenced workflow. Its inventory, policy, remediation, and reporting capabilities, grounded in DigiCert's own migration experience, illustrate a credible model for organizations of varying maturity to start building cryptographic visibility today, rather than wait for certainty about quantum computing timelines. Packaging discovery, policy, and remediation into one self-service preview reflects a bet that buyers want a starting point, not another framework document.

Potential challenge

DigiCert Quantum Central's principal marketplace challenge is differentiation and durability. Cryptographic discovery and posture management already draw competition from established governance, risk, and compliance (GRC), Continuous Threat Exposure Management (CTEM), and certificate lifecycle management vendors expanding into PQC readiness. As a preview offering with limited functionality, DigiCert must convert early free users into paying customers once general availability arrives, while proving that its inventory, policy, and remediation workflow scale across the fragmented, multi-vendor cryptographic environments many enterprises actually run, not just DigiCert-managed infrastructure.

Related research

- *Quantum Risk Is Already Here: An Enterprise Buyer's Guide to Assessing Third-Party Cryptographic Readiness Before Q-Day, Part 1 — Situation and Strategic Guidance* (IDC #US54672426, July 2026)
- *Quantum Risk Is Already Here: An Enterprise Buyer's Guide to Assessing Third-Party Cryptographic Readiness Before Q-Day, Part 2: Assessment Framework and Deployment Guide* (IDC #US54672526, July 2026)
- *Quantum Risk Is Already Here: A Provider's Guide to Demonstrating Third-Party Cryptographic Readiness Before Q-Day, Part 1 — Situation and Strategic Guidance* (IDC #US54672226, July 2026)
- *Quantum Risk Is Already Here: A Provider's Guide to Demonstrating Third-Party Cryptographic Readiness Before Q-Day, Part 2: Assessment Framework and Deployment Guide* (IDC #US54672326, July 2026)

Synopsis

This IDC Market Note examines DigiCert Quantum Central, a new solution within the DigiCert ONE portfolio previewed on July 1, 2026, to help organizations begin post-quantum cryptography readiness. DigiCert, which serves more than 125,000 organizations, including 90% of the Fortune 500, built Quantum Central to give security and IT teams a practical, self-service way to discover cryptographic assets, identify quantum-vulnerable systems, prioritize remediation, and track migration progress across fragmented, multi-vendor cryptographic environments toward a clearly defined readiness road map.

The note traces how Quantum Central's inventory, policy, remediation, and reporting workflow, informed directly by DigiCert's own internal migration experience, could reshape the broader PQC readiness marketplace and customer expectations around evidence-backed compliance posture. It also reviews the competitive challenges DigiCert faces in converting free preview users into paying customers as general availability approaches. It offers IDC's point of view on the solution's differentiation against established GRC, CTEM, and certificate lifecycle management vendors already active in the category.

"Quantum Central turns a vague mandate into a sequenced workflow," says Philip D. Harris, research director, Governance, Risk, and Compliance Solutions, IDC. "Visibility, not certainty, is the starting point."

ABOUT IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

Global headquarters

One Beacon Street
Suite 33100
Boston, MA 02108
USA
508.872.8200
X: @IDC
blogs.idc.com
www.idc.com

Copyright Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, and web conference and conference event proceedings. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit idc.com/about/offices. Please contact IDC at customerservice@idc.com for information on additional copies, web rights, or applying the price of this document toward the purchase of an IDC service.

Copyright 2026 IDC. Reproduction is forbidden unless authorized. All rights reserved.