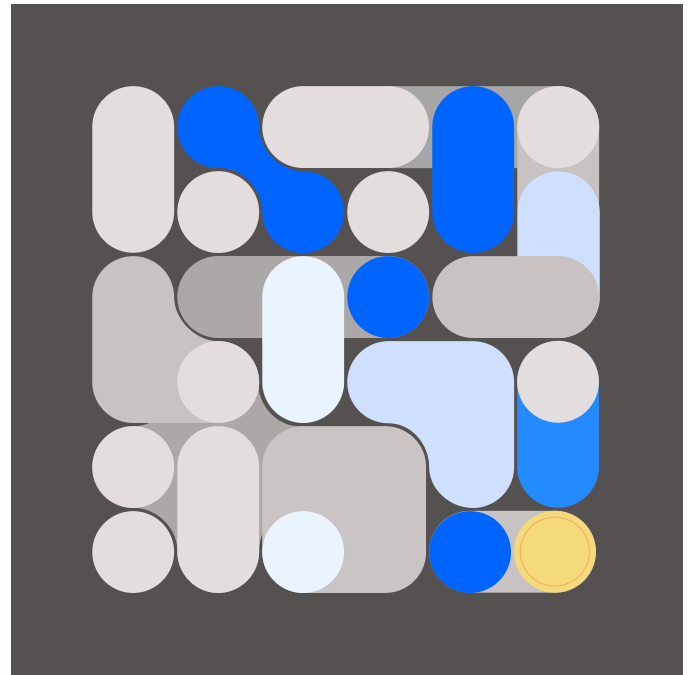


Achieve Crypto-Agility

Protect sensitive data, mitigate risk,
and prepare your organization for
quantum-resilience.



Quantum computing is coming

Rapid digital transformation is creating new challenges in the data security landscape. Organizations are struggling to manage cryptography and protect their sensitive data – looming quantum-safe deadlines from the National Institute of Standards and Technology (NIST) and others as well as threats from “harvest now, decrypt later” attacks mean action is required today. In addition to the quantum threat, security teams struggle with visibility, lifecycle management, and tool sprawl. As regulations evolve and threats emerge, organizations need cryptographic agility, or crypto-agility, to rapidly discover, monitor and update algorithms.

Protecting today. Preparing for tomorrow.

Crypto-agility – or the ability to rapidly adapt cryptographic mechanisms in response to threats, technological advances, or vulnerabilities, without disrupting infrastructure or business processes – is the solution to tackling today's challenges and building resilience against the quantum threat.

IBM Guardium® Cryptography Manager helps your organization achieve crypto-agility through discovery and inventory, risk assessment, cryptographic object lifecycle management, compliance-readiness, and protection of cryptographic objects. This enables you to manage cryptography at scale, reduce risk, and move toward quantum-safe resilience—all from one solution.

With IBM Guardium Cryptography Manager you can:

- **Discover and inventory** your cryptographic landscape to gain complete visibility. Identify cryptographic objects, detect unknown or shadow cryptography, map dependencies, ownership, and usage, and extend coverage through IBM Quantum Safe Explorer findings, Portfolio View, SSH public key discovery, and flexible imports from custom data sources.
- **Assess and comply** using a policy engine aligned to compliance standards. Evaluate post-quantum cryptography risk, flag outdated or vulnerable algorithms, map violations to internal and industry frameworks, and generate audit-ready reports that support HIPAA, PCI-DSS, and GDPR requirements.
- **Manage lifecycle** with automation that prevents outages. Centralize lifecycle operations in one tool, automate key generation, certificate renewal, and certificate deployment, enforce consistent policies across the organization, and accelerate remediation with AI-assisted ticket creation.
- **Protect and adapt** with a crypto-agile architecture that abstracts cryptography from applications, enabling organization-wide changes without disruption. Protect sensitive data with centralized encryption controls, evaluate the efficiency and feasibility of PQC algorithms, and defend against “harvest now, decrypt later” attacks.

Prepare your enterprise for quantum resilient cryptography through crypto-agility with IBM Guardium Cryptography Manager.

Reach out to your sales representative to learn more.

© Copyright IBM Corporation 2026. IBM, the IBM logo, and Guardium are trademarks or registered trademarks of IBM Corp., in the U.S. and/or other countries.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

