# IBM Guardium Cryptography Manager

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

**Highlights**

Discovery and inventory – gain comprehensive visibility

Policy and risk assessment – achieve faster compliance

Monitoring and reporting - turn insights into action

Flexible deployment and data ingestion

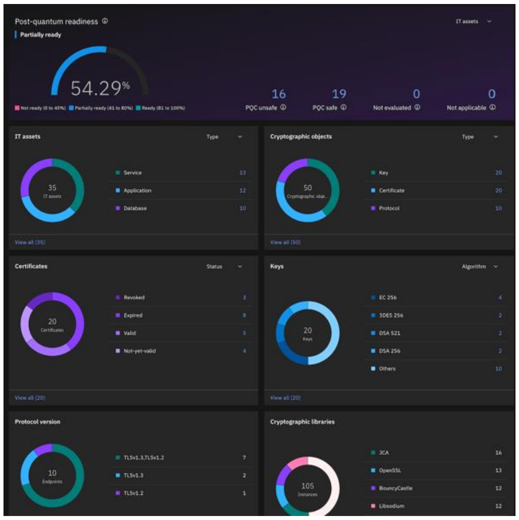
Remediation and role-based access

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.

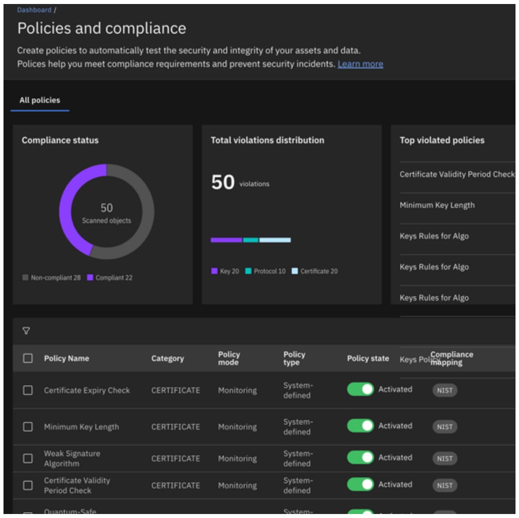
Crypto-agility – or the ability to rapidly adapt cryptographic mechanisms in response to threats, technological advances, or vulnerabilities, without disrupting infrastructure or business processes – is the solution to tackling today's challenges and building resilience against the quantum threat.

IBM Guardium® Cryptography Manager helps your organization achieve crypto-agility through discovery and inventory, risk assessment, cryptographic object lifecycle management, compliance-readiness, and remediation 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, and map dependencies, ownership, and usage.
— Assess and comply using a policy engine aligned to compliance standards. Evaluate post-quantum cryptography risk and flag outdated or vulnerable algorithms.
— Prioritize vulnerabilities according to business risk, enable remediation to expedite response and generate audit-ready reports.



Guardium Cryptographic Manager dashboard



Policies and compliance

Create policies to automatically test the security and integrity of your assets and data.
Polices help you meet compliance requirements and prevent security incidents. Learn more

| □ | Policy Name | Category | Policy mode | Policy type | Policy state | Compliance mapping |
|---|---|---|---|---|---|---|
| □ | Certificate Expiry Check | CERTIFICATE | Monitoring | System-defined | Activated | NIST |
| □ | Minimum Key Length | CERTIFICATE | Monitoring | System-defined | Activated | NIST |
| □ | Weak Signature Algorithm | CERTIFICATE | Monitoring | System-defined | Activated | NIST |
| □ | Certificate Validity Period Check | CERTIFICATE | Monitoring | System-defined | Activated | NIST |
| □ | Quantum-Safe | | | System- | | |

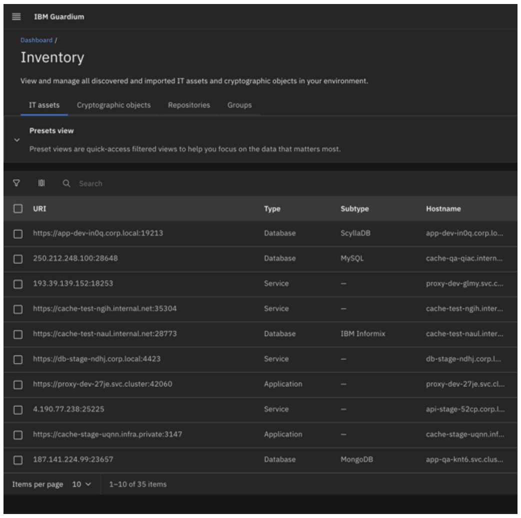
Policies and compliance

### Discovery and inventory – gain comprehensive overview

IBM Guardium Cryptography Manager discovers data from diverse sources and formats to build a complete picture of your environment. It identifies IT assets and their associated cryptographic objects across the enterprise, then presents detailed insights for each discovery, including type, subtype, location, and identifiers. The platform collects and displays rich metadata for cryptographic objects—such as algorithm, expiration date, issuer details, and usage context—and consolidates IT assets, cryptographic objects, and repositories into a single inventory. That inventory is enriched with violation findings and cryptographic usage data from IBM Quantum Safe Explorer and network scans, and it models clear relationships between assets and their cryptographic objects to simplify risk management and compliance, for example mapping servers to their SSL/TLS certificates.

### Policy and risk assessment – achieve faster compliance

The solution creates and manages policies to evaluate risks and violations at scale. It includes system-defined policies aligned to National Institute of Standards and Technology (NIST) guidance and supports customized rule-based policies through a built-in policy wizard. Guardium Cryptography Manager analyzes assets and cryptographic objects for adherence to these policies, producing violations that can be categorized as classical or post-quantum cryptography (PQC) issues. It highlights critical risks with alerts, assigns exploitability scores, and flags misconfigurations. Each evaluated asset receives an exploitability score derived from associated cryptographic objects—such as certificates, keys, protocols, and cipher suites—using CVSS metrics.



Inventory

View and manage all discovered and imported IT assets and cryptographic objects in your environment.

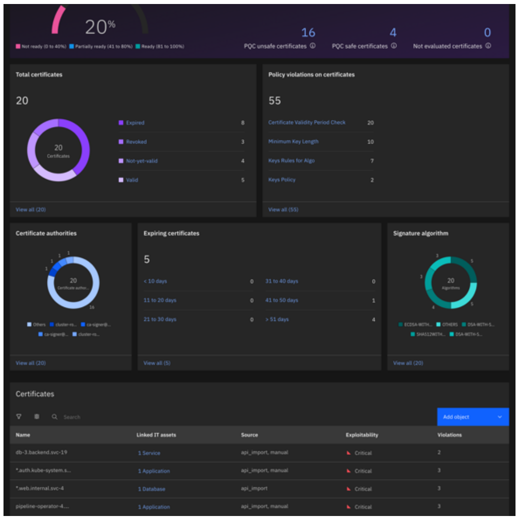
Presets view

Preset views are quick-access filtered views to help you focus on the data that matters most.

| URI | Type | Subtype | Hostname |
|---|---|---|---|
| https://app-dev-in0q.corp.local:19213 | Database | ScyllaDB | app-dev-in0q.corp.lo... |
| 250.212.248.100:28648 | Database | MySQL | cache-qa-qiac.intern... |
| 193.39.139.152:18253 | Service | – | proxy-dev-glmy.svc.c... |
| https://cache-test-ngih.internal.net:35304 | Service | – | cache-test-ngih.inter... |
| https://cache-test-naul.internal.net:28773 | Database | IBM Informix | cache-test-naul.inter... |
| https://db-stage-ndhj.corp.local:4423 | Service | – | db-stage-ndhj.corp.l... |
| https://proxy-dev-27je.svc.cluster:42060 | Application | – | proxy-dev-27je.svc.cl... |
| 4.190.77.238:25225 | Service | – | api-stage-52cp.corp.l... |
| https://cache-stage-uqnn.infra.private:3147 | Application | – | cache-stage-uqnn.inf... |
| 187.141.224.99:23657 | Database | MongoDB | app-qa-knt6.svc.clus... |

Items per page 10 1–10 of 35 items

Inventory dashboard



| Name | Linked IT assets | Source | Exploitability | Violations |
|---|---|---|---|---|
| db-3.backend.svc-19 | 1 Service | api_import, manual | Critical | 2 |
| *.auth.kube-system.s... | 1 Application | api_import, manual | Critical | 3 |
| *.web.internal.svc-4 | 1 Database | api_import | Critical | 3 |
| pipeline-operator-4.... | 1 Application | api_import, manual | Critical | 3 |

Certificates dashboard

### Monitoring and reporting - turn insights into action

IBM Guardium Cryptography Manager continuously monitors cryptographic data through interactive dashboards and generates exportable reports. Dashboards track cryptographic object distribution, expiry trends, and algorithm usage, while logs provide actionable insights into posture and guide remediation decisions. Reports summarize inventory, violations, and overall risk to support audits and executive briefings.

### Flexible deployment and data ingestion

IBM Guardium Cryptography Manager supports installation through Helm on Kubernetes clusters or on Red Hat OpenShift Container Platform.
The solution installs via Helm on Kubernetes clusters or on Red Hat OpenShift Container Platform. It ingests data from a wide range of sources, including network scanners and Kubernetes; Vault for certificate discovery; Qualys and Nessus for IT and cryptographic assets; Cryptographic Bill of Materials (CBOM) for code assets; and IBM Quantum Safe™ Explorer for code vulnerabilities and post-quantum readiness assessments. It also supports preformatted file imports, with CSV uploads in the user interface and JSON ingestion through APIs for bulk data from external tools.

### Remediation and role-based access

IBM Cryptography Manager integrates with ticketing systems such as Jira and ServiceNow to streamline remediation workflows from detection through closure. Role-based access ensures appropriate control, with capabilities available to Super Administrator, Compliance Officer, Security Administrator, and Database Administrator roles.

## IBM Guardium Cryptography Manager system requirements

| **Kubernetes cluster requirements nodes** | **vCPU Cores** | **Memory in GB** | **Storage in GB** |
|---|---|---|---|
| Control plane node 1, 2, 3 | 2 | 4 | 30 |
| Worker node 1, 2, 3 | 8 | 16 | 50 |
| **OCP cluster requirements nodes** | | | |
| Control plane node 1, 2, 3 | 4 | 16 | 100 |
| Worker node 1, 2, 3 | 8 | 16 | 100 |
| Bootstrap (reclaimed later) | 4 | 16 | 100 |
| **Browser recommendations:**<br>Google Chrome incognito mode<br>Mozilla Firefox incognito mode | | | |

IBM Guardium Cryptography Manager is a unified, AI-powered solution that helps your organization protect sensitive data, mitigate risk, achieve crypto-agility, and build toward quantum resilience. It delivers comprehensive visibility through discovery and inventory and streamlines risk assessment and compliance. Prepare your enterprise for quantum resilient cryptography through crypto-agility with IBM Guardium Cryptography Manager.

**For more information**

To learn more about the solution, contact your IBM representative or IBM Business Partner.

Produced in the
United States of America
September 2025

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.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided.