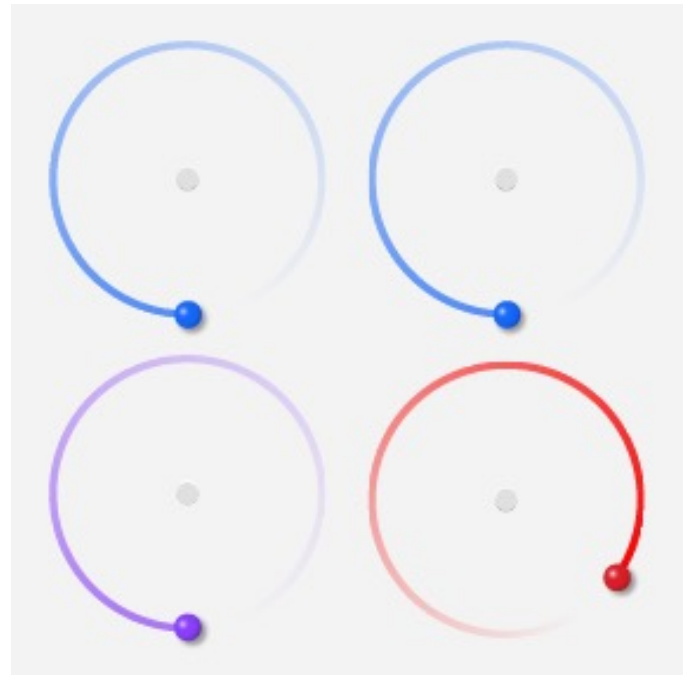# IBM Guardium Quantum Safe

Gain visibility into your cryptographic posture. Assess and prioritize cryptographic vulnerabilities to secure your critical data.

Traditional encryption methods may soon be "broken."

Data security is the foundation of every business transaction. For decades, enterprises have relied on standard cryptography and encryption methods to safeguard their data, applications, and endpoints. As quantum computing advances, all sensitive information secured by today's encryption standards and practices may become vulnerable. What would take conventional computers centuries to break could be cracked within hours using quantum computing, exposing sensitive data and putting businesses at risk.

IBM®, who developed two recently published NIST post-quantum cryptographic standards[1] in collaboration with industry partners, is a leader in the Quantum Safe space. IBM Guardium® Quantum Safe™ monitors your enterprise's cryptography use, uncovers cryptographic vulnerabilities, and prioritizes remediation to secure your data from both conventional and quantum-enabled risks.

Comprehensive, consolidated visibility
Gain enhanced visibility into your organization's cryptographic posture, vulnerabilities, and remediation progress

Help enable faster compliance
Users can define and enforce policies based on internal security policies and external regulations, as well as integrate with enterprise issue tracking tools

Prioritize vulnerabilities to accelerate remediation
Investigate violations and prioritize for remediation based on contextual insights

Guardium Quantum Safe leverages both IBM's leadership in quantum research and deep expertise in data security. Learn more about how to secure your organization for the quantum era.

Contact your IBM representative to get started.