IBM **Quantum**

IBM Quantum Safe technology

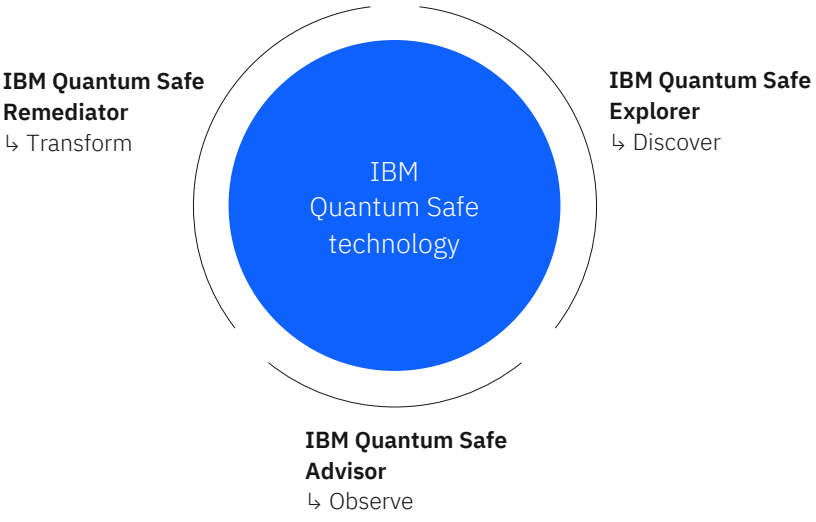
Safeguard your data and modernize your cryptography for the quantum era

A comprehensive solution for your quantum-safe journey

Quantum computing promises immense business value for clients, but quantum computers will also be able to break some of the most widely used security protocols in the world. Businesses face an imperative to understand the risk quantum technology poses to their systems and data, develop a quantum-safe strategy, and help their teams build competency in quantum-safe cryptographic implementations.

IBM Quantum Safe is a comprehensive set of tools, capabilities, and approaches combined with deep expertise to help you plan and execute your organization's migration to quantum-safe cryptography. Build quantum cyber resilience in three phases—Discover, Observe, and Transform—each powered by IBM Quantum Safe technology.

A comprehensive solution for your quantum-safe journey



Discover

Identify cryptography usage, analyze dependencies, and generate Cryptography Bill of Materials (CBOM).

Observe

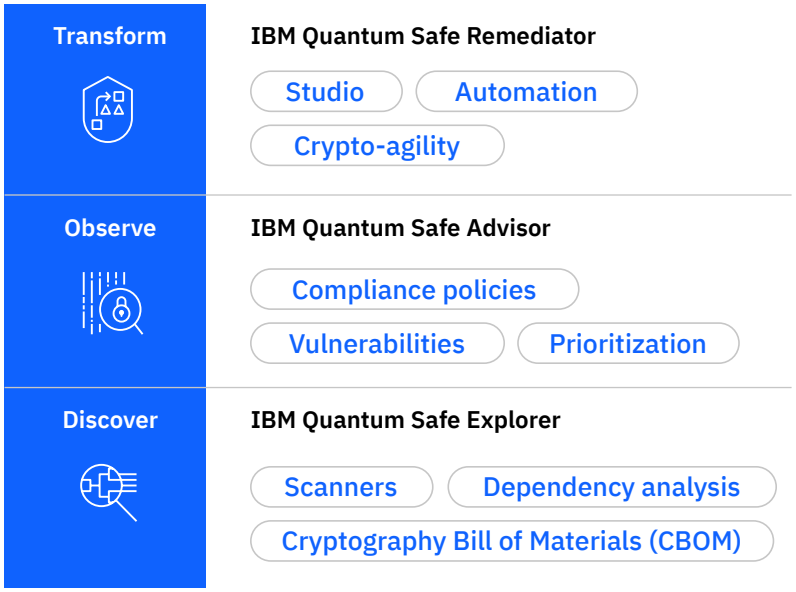
Analyze cryptographic posture of compliance and prioritize vulnerabilities based on risks. Track KPIs for cryptographic modernization.

Transform

Remediate vulnerabilities using quantum-safe best practices. Learn, explore, and implement quantum-safe cryptography to achieve crypto-agility.

An end-to-end approach to achieving crypto-agility

IBM Quantum offers an end-to-end solution to help organizations plan an efficient and secure migration from today's classical cryptography to tomorrow's quantum-safe cryptography, regardless of where they are starting from.



The time to prepare is now

Data not secured today is already lost
The quantum era will unfold over time, but "harvest now, decrypt later" attacks enable cybercriminals to steal data today and store it until more advanced quantum computers emerge.

Rising cost of data breaches
Reaching an all-time high, the cost of a data breach averaged USD 4.35 million in 2022, a 12.7% increase from 2020.[1] This figure is likely to increase further as quantum-based attacks become more common.

Shortage of skills
CISOs and CIOs are becoming aware of the approaching threat of quantum-based attacks but may not know how to protect against them.

Impending regulation
Governments and regulatory bodies around the world are monitoring developments in quantum technology and are beginning to establish timelines and guidelines for the transition to quantum-safe cryptography.

1. IBM Security. "Cost of a Data Breach Report 2022." IBM, 2022.

For more information about IBM Quantum Safe technology, visit: **https://www.ibm.com/quantum/quantum-safe**

Technology overview

IBM Quantum Safe Explorer

IBM Quantum Safe Explorer scans and analyzes source code and object code to identify all cryptographically relevant artifacts, uncover dependencies, and surface vulnerabilities. Explorer also generates a Cryptography Bill of Materials (CBOM), a common extension to the software supply chain that offers a systematic way of mapping dependencies between protocols and cryptography libraries, providing a breakdown of cryptographic algorithms that are used and vulnerable libraries that need to be fixed.

IBM Quantum Safe Advisor

IBM Quantum Safe Advisor performs an enterprise-wide cryptography analysis and builds a comprehensive cryptographic inventory that details the types and locations of your cryptographic instances; the cipher suites, certificates, and CBOMs associated with assets; the relationships between assets and data flows; and potential vulnerabilities. Advisor also gives you the ability to sort your inventory based on internal classification criteria, enabling you to generate a prioritized list of non-quantum-safe cryptography.

IBM Quantum Safe Remediator

IBM Quantum Safe Remediator helps you to create an architecture for seamlessly upgrading your cryptography infrastructure to quantum safe through a robust set of remediation patterns based on enterprise use cases.