

IBM **Quantum** Safe

IBM Quantum Safe → **Technology**

Safeguard your data and modernize
your cryptography for the quantum era



A comprehensive solution for your quantum-safe journey

IBM Quantum Safe technology enables you to discover, observe, and transform cryptography while building crypto-agility

Quantum computing promises immense business value for clients, but it 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 and develop a quantum-safe strategy.

The time to prepare is now

Data not secured today is already lost

Although a cryptographically relevant quantum computer does not yet exist, “harvest now, decrypt later” attacks could enable cybercriminals to steal data today and store it until more advanced quantum computers emerge.

Rising cost of data breaches

The average cost of a data breach reached an all-time high in 2023 at USD 4.45 million.¹ This figure is likely to increase further as quantum-based attacks become more common.

Shortage of skills




Security leaders are becoming aware of the approaching threat of quantum-based cyberattacks but may lack teams with competency in quantum-safe cryptographic implementations

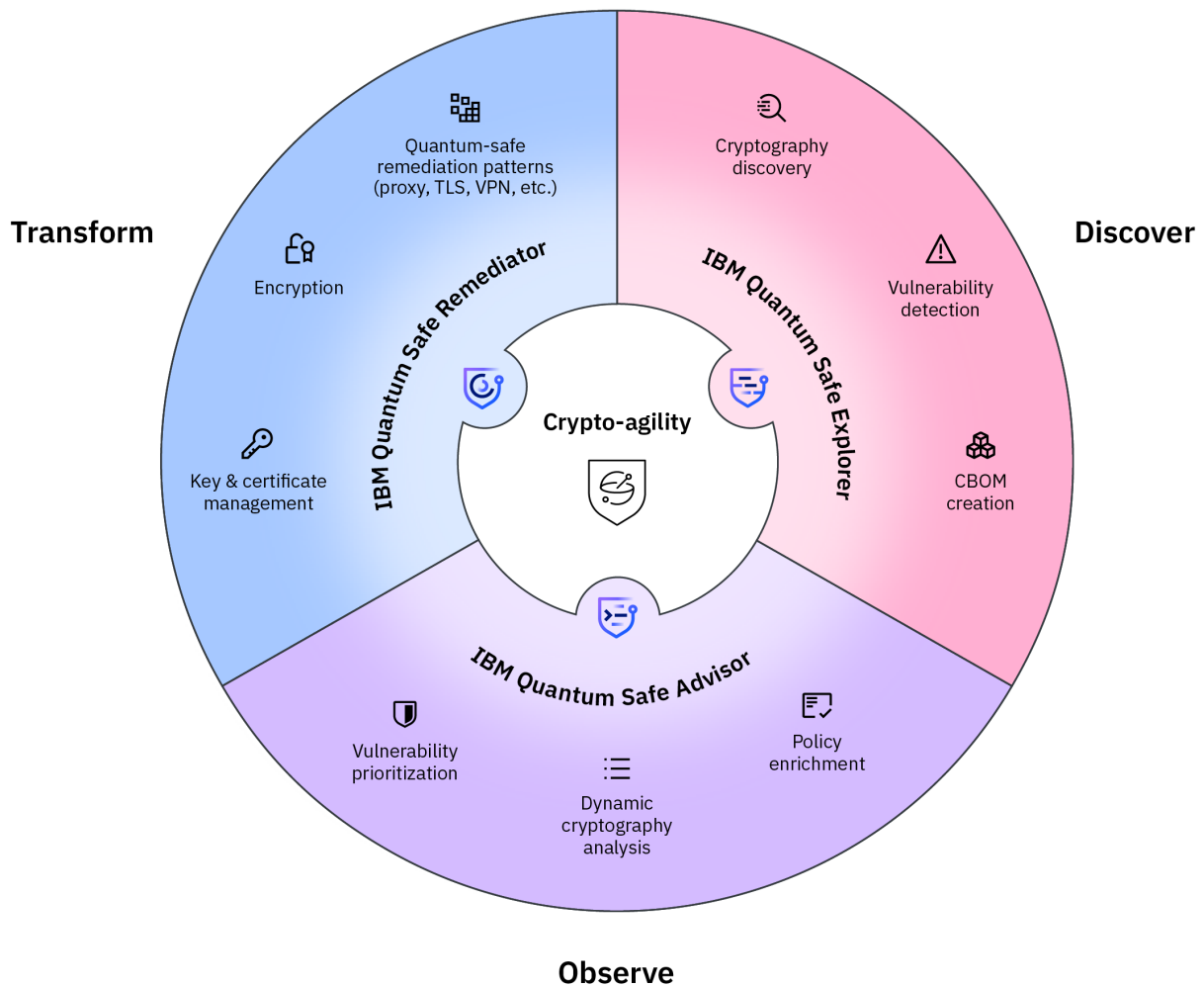
Impending regulation

Governments and regulatory bodies around the world are beginning to establish guidelines and timelines for transitioning to quantum-safe cryptography.

IBM Quantum Safe technology

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, each powered by IBM Quantum Safe technology:

| | |
|------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
|  Discover | Identify cryptography usage, analyze dependencies, and generate Cryptography Bills of Materials (CBOMs). |
|  Observe | Analyze cryptographic posture of compliance and prioritize vulnerabilities based on risks. |
|  Transform | Remediate vulnerabilities using quantum-safe best practices. Implement quantum-safe cryptography to achieve crypto-agility. |



IBM Quantum Safe Explorer

Explorer scans and analyzes source code and object code to identify cryptographically relevant artifacts and surface vulnerabilities. Explorer also generates a cryptographic inventory in a variety of formats, including 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.

IBM Quantum Safe Advisor

Advisor performs an enterprise-wide cryptography analysis to determine 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 enables you to evaluate your cryptographic posture of compliance, enabling you to generate a prioritized list of at-risk cryptographic assets.

IBM Quantum Safe Remediator

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.

For more information about IBM Quantum Safe technology, visit <https://www.ibm.com/quantumsafe> or scan the QR code below.



1. IBM Security. "Cost of a Data Breach Report 2023." 2023.

