

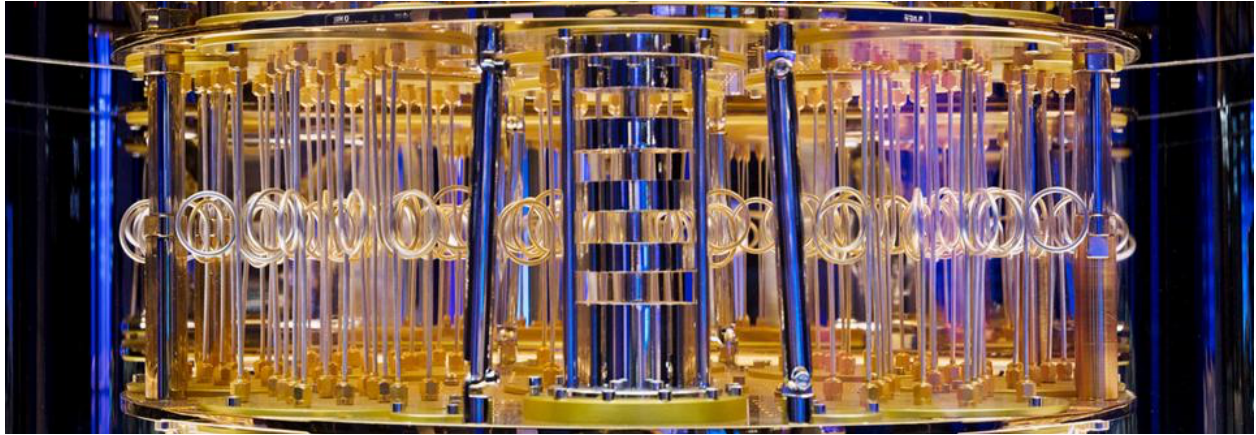
# IBM Helps Clients Prepare for a Quantum-Safe World

***IBM unveils new software to help clients protect data that someday could become threatened by quantum code-breakers.***

Quantum computing has the potential to create immense business benefits, and the social implications of quantum technologies are likely to be far-reaching. By decade's end, practical quantum computing solutions could impact computing strategies across industries. Over upcoming investment cycles, quantum computing will profoundly alter how we think of computing and, critically, how we secure our digital economy through cryptography.

## Why Quantum Safe Now?

Developing “quantum-safe” cryptography capabilities is crucial to maintaining data security and integrity for critical applications. The quantum era will unfold over time, but the need for quantum-safe solutions is immediate. There is significant concern that data considered securely protected today could already be lost to a future quantum adversary. “Steal now, decrypt later” strategies of bad actors can be prevented by developing new cryptography approaches that are immune from attacks from future quantum computers.



An IBM Quantum Computer.

Since all data – past, present, and future – that is not protected using quantum-safe security may one day be at risk, it follows that the longer that the migration to quantum-safe standards is postponed, the more data remains potentially insecure. Business, technology, and security leaders face an urgent need to develop a quantum-safe strategy and roadmap now. In fact, both the historic and current complexity of cryptography migrations—even pre-quantum computing—can require several years of strategic planning, remediation, and transformation.

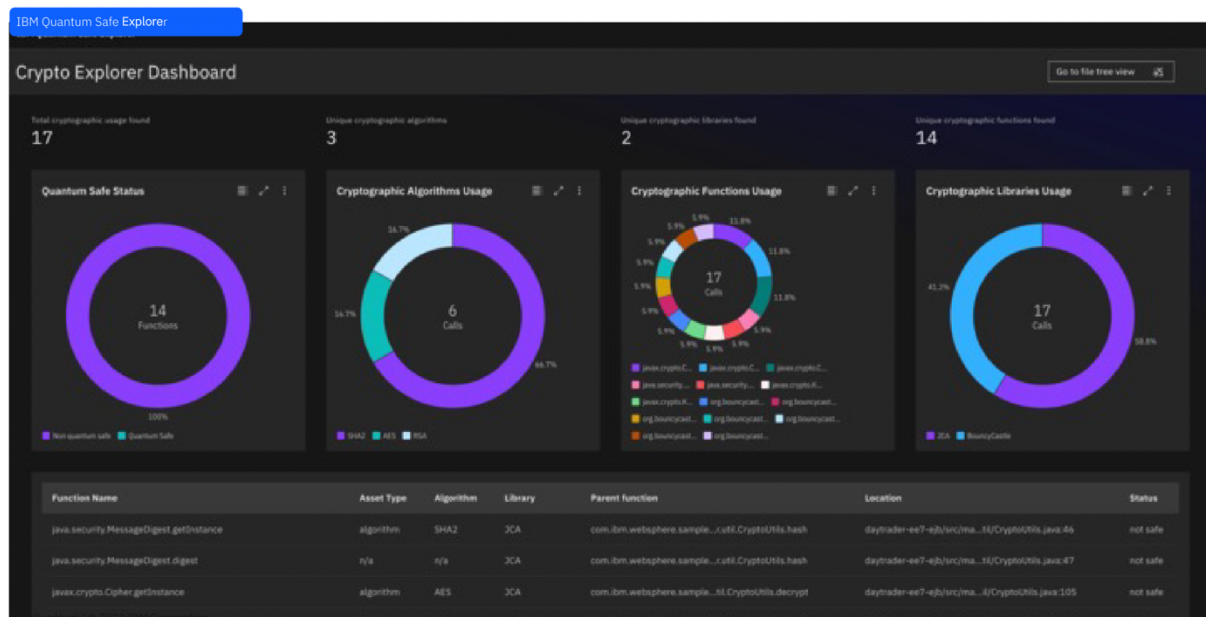
One of IBM's advantages in pioneering quantum-safe cryptography is its expertise in both quantum computing and classical cryptography. IBM has been at the forefront of quantum computing research and has developed one of the most advanced quantum computing platforms, IBM Quantum. This gives IBM unique insight into the potential impact of quantum computing on cryptography and the ability to develop and test new quantum-safe cryptographic systems.

# What is New From IBM?

In its latest step forward, IBM is unveiling its IBM Quantum Safe technology to empower customers throughout their journey to quantum safe. The new offerings include:

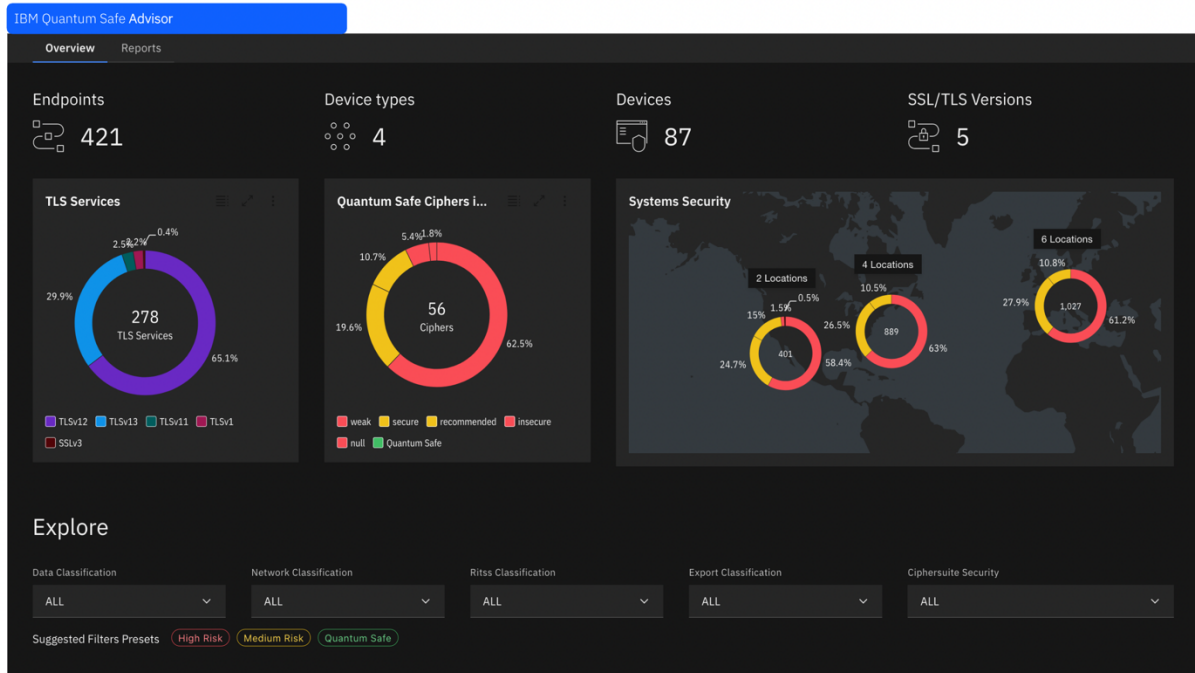
- **IBM Quantum Safe Explorer:** helps customers discover their cryptography by scanning source code and object codes, analyzing dependencies and generating Cryptography Bill of Material (CBOM).

## IBM Quantum Safe Explorer



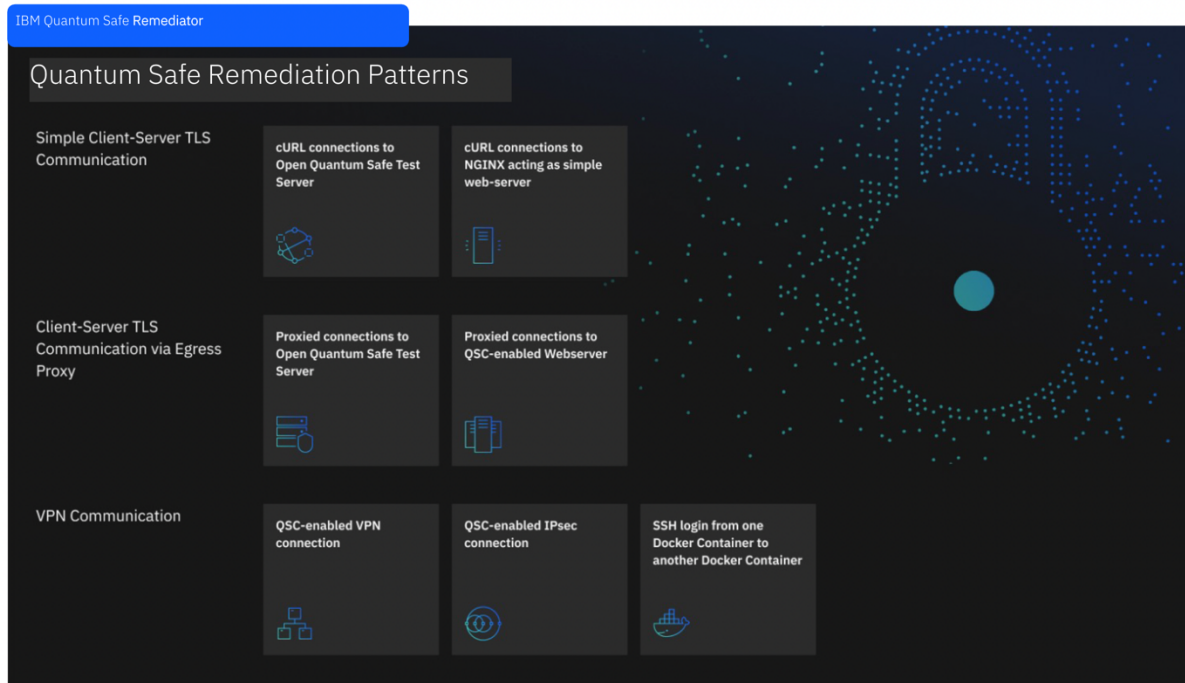
- **IBM Quantum Safe Advisor:** helps customers observe their cryptography by analyzing their compliance posture, vulnerabilities across the cryptography assets, and prioritizing the remediation based on risk.

# IBM Quantum Safe Advisor



- **IBM Quantum Safe Remediator:** helps customers transform their cryptography by providing crypto-agility with best-fit remediation patterns while reducing development and operation burden for implementation and deployment.

# IBM Quantum Safe Remediator



These three capabilities can provide a comprehensive end-to-end solution for clients to transform their applications to become quantum safe. The need to do so is immediate, and clients should begin this effort as soon as possible to avoid the costly security breaches that quantum computing will enable soon.

## Conclusions

Overall, IBM's expertise in both quantum computing and classical cryptography, its involvement in the development of quantum-safe cryptographic standards, and its collaborative approach to innovation give it a significant advantage in pioneering quantum-safe cryptography. IBM is intent on helping their clients protect their data and infrastructure now, and offers the technologies and expertise needed to do so.