IBM Quantum Safe Explorer

Simplify the discovery of cryptography and the management of quantum security risks.

Highlights
Scan applications to rapidly locate cryptographic artifacts

Systematize static code inventory and analysis with the creation of Cryptography Bills of Materials (CBOMs)

Seamlessly integrate static code analysis and editing with automated tooling that fits into your CI/CD cycle

With quantum technology rapidly advancing, the need to secure your digital applications against cyberattacks involving future cryptographically relevant quantum computers has become more pressing. Cybercriminals could already be using “harvest now, decrypt later” attacks to steal and store data until they can decrypt it. Protecting your assets now and in the future requires a migration to quantum-safe cryptographic algorithms—a process that begins with discovering where cryptography is being used in your applications. But locating cryptography within applications is like searching for a needle in a haystack: for an application with 20,000 lines of code, there may be half a dozen instances of cryptography.

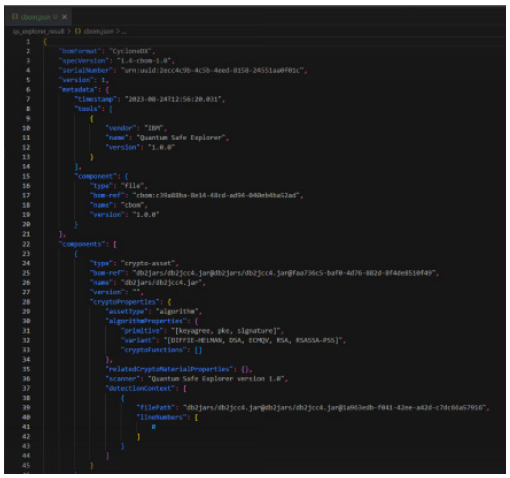
IBM Quantum Safe Explorer streamlines the cryptographic discovery process and provides you with a static view of your cryptography usage and quantum security risks. Explorer enables you to:

Rapidly locate cryptographic occurrences.
Scan source code to identify calls to commonly used cryptographic libraries, and surface potential vulnerabilities to quantum technology.

Simplify application vulnerability management.
Generate a Cryptography Bill of Materials (CBOM), an extension to the software supply chain that systematizes the creation and sharing of metadata describing cryptographic artifacts.

Automate static code analysis and reporting.
Integrate Explorer within your development environment and CI/CD pipeline so that you can edit code, rescan, and instantly validate the application’s upgraded security.

Sign up to view a live demo at https://ibm.com/quantumsafe.



A Cryptography Bill of Materials (CBOM) produced by IBM Quantum Safe Explorer.

Cryptography Bill of Materials (CBOM)

A Cryptography Bill of Materials (CBOM) is a schema extension of the CycloneDX Software Bill of Materials (SBOM) that provides an object model for describing cryptographic artifacts and their dependencies. With its automated tooling, Explorer creates a CBOM that can be shared with your software supply chain and updates the file every time you rescan your application. By formatting metadata related to cryptographic components using an easily consumable method, the CBOM enables you to incorporate cryptography lifecycle management efficiently into your software supply chain risk management processes.

Learn more about the CBOM schema at https://github.com/IBM/CBOM.

Begin your quantum-safe transition

Take the next steps to learn more about IBM Quantum Safe Explorer and the benefits of quantum-safe application management. Get started today at https://ibm.com/quantumsafe.

IBM Quantum Safe Explorer

IBM Quantum Safe Explorer provides two modes of operation:
1. A backend service (API) and a Visual Studio Code extension as a user interface that are installed locally on your system.
2. A stand-alone command-line interface (CLI) that runs locally on your system.

User interface	Visual Studio Code extension	CLI	API
System requirements	**IBM Quantum Safe Explorer service:** • Oracle JDK or Open JDK 17 or higher • 16 GB RAM minimum on MacOS (Ventura on Intel and M1) or Windows 11 **Front-end interface:** • Visual Studio Code 1.77 or higher	• Oracle JDK or Open JDK 17 or higher • 16 GB RAM minimum on MacOS (Ventura on Intel and M1) or Windows 11	• Oracle JDK or Open JDK 17 or higher • 16 GB RAM minimum on MacOS (Ventura on Intel and M1) or Windows 11
Languages supported	• Java/Jar • Dart • Python • C/C++	• Java/Jar • Dart • Python • C/C++	• Java/Jar • Dart • Python • C/C++
Cryptography libraries supported	Java • BouncyCastle • Java Cryptography Architecture (JCA)	Java • BouncyCastle • Java Cryptography Architecture (JCA)	Java • BouncyCastle • Java Cryptography Architecture (JCA)
	Dart • Cryptography	Dart • Cryptography	Dart • Cryptography
	Python • Crypto • Cryptography	Python • Crypto • Cryptography	Python • Crypto • Cryptography
	C/C++ • Crypto++ • OpenSSL • Open Quantum Safe (OQS)	C/C++ • Crypto++ • OpenSSL • Open Quantum Safe (OQS)	C/C++ • Crypto++ • OpenSSL • Open Quantum Safe (OQS)

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
September 2023