IBM Quantum Safe Explorer

Discover application cryptographic vulnerabilities to plan, budget, and prioritize remediation.

Highlights

Portfolio View - Centralize cryptography management

Generate Cryptography Bill of Materials (CBOM)

API Discovery Crypto-Inventory - Simplify crypto-function discovery

Parameter tracing – Identify bad coding practices

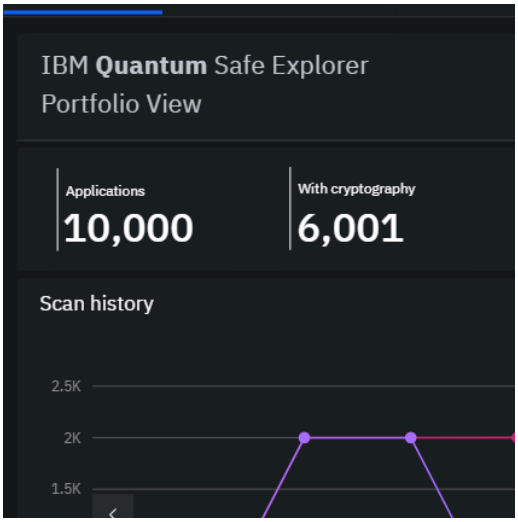
IBM Quantum Safe Explorer compliance

IBM Quantum Safe Explorer system requirements

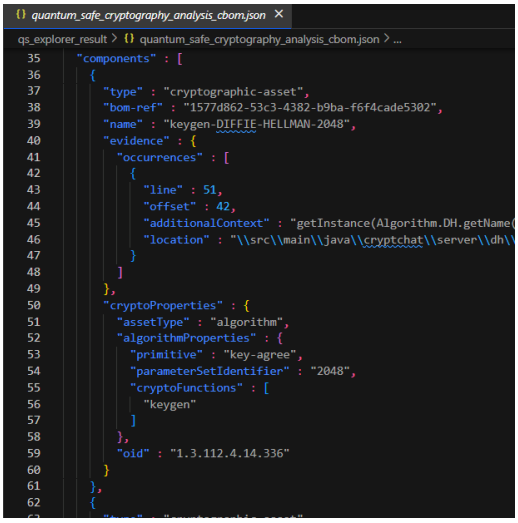
The acceleration of the quantum era introduces an urgent cybersecurity challenge. Cybercriminals are already using “harvest now, decrypt later” tactics—collecting encrypted data today to exploit once quantum capabilities mature. In 2024, the National Institute of Standards and Technology (NIST) certified new encryption standards to modernize cybersecurity, helping enterprises, government agencies, and technology vendors build resilience. In November 2024, NIST issued a draft report affirming that non-quantum-safe cryptographic algorithms, such as RSA, will be considered disfavored by 2030. As a result, post-quantum cryptographic migration is becoming a global priority. The Monetary Authority of Singapore (MAS), the U.S. White House, and 18 EU member states emphasize the need for tracking cryptographic assets, while PCI DSS will mandate an updated inventory by March 2025. Additionally, regulations like the EU’s Digital Operations Resilience Act (DORA) underscore the importance of cryptographic agility and the transition to quantum-safe protocols to ensure data security.

Hence, a key step is building an inventory of cryptography in use. With organizations managing thousands of homegrown applications and libraries, locating cryptographic assets across complex codebases is like finding a needle in a haystack.

IBM Quantum Safe™ Explorer simplifies the discovery and management of cryptographic vulnerabilities within enterprise applications by performing source code scanning to identify cryptographically relevant artifacts that may be vulnerable to quantum attacks. Explorer identifies all the relevant cryptographic asset types, variants and primitives used within the supported programming languages. Explorer then presents the cryptographic findings in the portfolio view to help clients draw actionable insights that transform cryptographic management from chaos to clarity. The timely detection of cryptographic vulnerabilities enables CIOs, CISOs, and security analysts to detect vulnerabilities, and prioritize remediation efforts with confidence to fortify the enterprise for the quantum era.



Portfolio view



CBOM generation

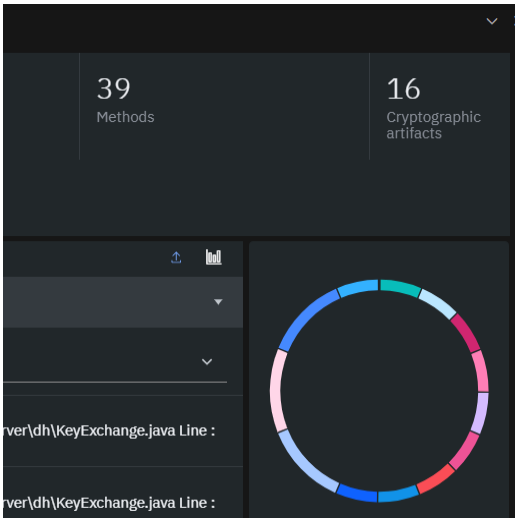
Portfolio view - Centralize cryptography management

The Portfolio View offers a comprehensive overview of cryptographic vulnerabilities across the enterprise applications. By aggregating scan results, this feature provides an interactive dashboard to easily assess risks across applications and business units. With clear visualizations and drill-down capabilities, CIOs or CISOs can quickly identify critical vulnerabilities, prioritize remediation, and ensure quantum-safe compliance. The dashboard categorizes vulnerabilities by severity—Minor, Major, and Critical—enabling efficient risk management and supports audit requirements. By centralizing cryptographic data, the Portfolio View simplifies decision-making, allowing security teams to plan, budget, and reduce exposure.

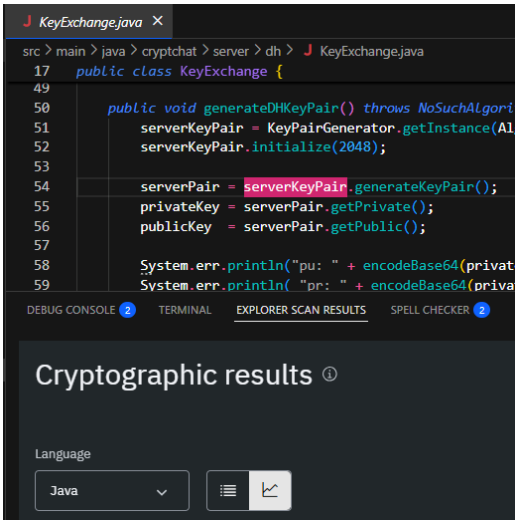
Generate Cryptography Bill of Materials (CBOM)

The CBOM is a groundbreaking extension of the CycloneDX 1.6 Software Bill of Materials (SBOM) standard, designed to bring structure and clarity to cryptographic asset management. By providing a detailed abstraction to model cryptographic assets—including algorithms, protocols, certificates, and cryptographic libraries—CBOM simplifies the daunting task of identifying and managing cryptographic dependencies across complex systems and applications. It captures critical asset properties, such as algorithm families and variants, enabling precise identification of vulnerabilities like weak algorithms (e.g., SHA-1). By mapping “uses” and “implements” relationships, CBOM delivers unparalleled insight into how cryptographic assets are embedded within software components, applications, and libraries.

CBOM seamlessly integrates into the broader software supply chain security ecosystems, making it an essential tool for enterprises preparing for quantum-safe migration. Its ability to automate reasoning about cryptographic compliance ensures that security teams can act faster and smarter, transforming cryptographic management from a reactive process into a proactive strategy.



API Discovery



Parameter tracing

API Discovery Crypto-Inventory - Simplify crypto-function discovery

The API discovery crypto-inventory feature addresses the challenge of identifying crypto-relevant code across large codebases. For organizations managing thousands of applications, it's difficult to know where cryptographic functions are implemented. This tool provides clear visibility by scanning code for cryptographic functions, pinpointing their locations, and generating a detailed inventory. Flat crypto-inventory helps CISOs and security teams focus their efforts by narrowing down to the pool of applications containing cryptographic functions, making deeper analysis more efficient. The feature scans various programming languages (e.g., C#, C++, Python, Go) and categorizes cryptographic functions by language and library, generating a comprehensive JSON-based list.

Parameter tracing – Identify bad coding practices

Cryptographic vulnerabilities often stem from improper API usage, hardcoded keys, or weak algorithms buried deep in the codebase. For DevSecOps teams, uncovering these issues is critical to mitigating risks and ensuring secure application development. Parameter tracing simplifies this process by mapping all cryptographic operations, from cipher.doFinal to cipher.init, cipher.getInstance, and key generation methods like generateAesKey.

This precise tracing ensures no cryptographic asset is overlooked, enabling security analyst to assess risks quickly, to detect bad coding practices, and to pinpoint and remediate vulnerabilities at the exact lines of code. By embedding parameter tracing into development workflows, organizations strengthen secure coding practices and streamline remediation.

IBM Quantum Safe Explorer compliance

IBM Quantum Safe Explorer performs compliance checks to ensure cryptographic algorithms are secure and meet regulatory standards. It verifies whether algorithms used are resistant to quantum attacks and reports compliance for each cryptographic asset identified during the Cryptography Analysis scan. If the algorithm property is unknown, the compliance status is marked as Unknown.

In addition, the solution checks for Federal Information Processing Standard 140-3 Level 1 (FIPS140-3-L1) compliance by validating that algorithms, modes, key lengths, curves, and moduli align with approved standards. These checks are applied only when algorithm properties are known; otherwise, the status remains Unknown. All compliance results are presented in the standalone IBM Quantum Safe Explorer Insights viewer for easy interpretation and action.

Results visualization

The results are displayed in the standalone IBM Quantum Safe Explorer Insights viewer for easy interpretation. As an alternative to the VS Code viewer, this utility enables users to explore cryptographic findings through an intuitive Insight Dashboard interface.

IBM Quantum Safe Explorer system requirements

IBM Quantum Safe Explorer has four components: backend service, user interface (VSCE), command-line interface (CLI), and Portfolio View.

	CLI/ Service / Visual Studio Code Extension		Portfolio View
System requirements	macOS Sonoma (Ventura on Intel, M1 or higher) or Windows 11 16GB RAM minimum, 32GB RAM recommended IBM Z Linux - command-line interface (CLI) only		Windows Server 2022 Standard or Red Hat Enterprise Linux (RHEL) 9 64 GB RAM, 16 vCPU
Software requirements	Oracle JDK 17.0.0, Open JDK 17.0.0, or higher Visual Studio Code 1.77 or higher Browser compatibility with Firefox, Chrome, Safari, Windows Edge (all versions)		Node.js v16 PostgreSQL 16.0 or higher IBM Cognos Analytics 12.0.4
Languages and cryptography libraries supported	C/C++	Crypto++, GSKit-crypto, liboqs, OpenSSL	
	C#	.NET cryptography library	
	Dart	Cryptography	
	Go	crypto, hash	
	Java	Bouncy Castle 1.77, Java Cryptography Architecture (JCA), Nimbus JOSE + JWT 10.2, Apache Commons Codec 1.18.0, JJWT :: API 0.11.0	
	Phyton	Crypto (PyCryptodome), cryptography, hashlib	

IBM Quantum Safe Explorer identifies all cryptographically relevant artifacts in supported languages across all environments and applications, including home-grown, and visualizes the findings in a centralized portfolio view. This helps you draw actionable insights, prioritize remediation, and build quantum resilience today.

For more information

To learn more about our quantum-safe solutions, contact your IBM representative or IBM Business Partner, or visit ibm.com/products/guardium-quantum-safe

Produced in the
United States of America
October 2025