



Future-Proof Data Exposure Risks for the Post-Quantum Era



The threat of quantum computing

Advances in quantum computing will render most widely used public key cryptographic algorithms obsolete. There is a high risk that within 5-10 years, quantum computers will be able to break most of today's public key cryptography, enabling unauthorized access to the sensitive data it currently protects.

Governments and private organizations are already taking action to prepare for the inevitable. Stronger, quantum-resistant algorithms are already available, and NIST will soon release new standards for encryption use cases such as key exchange, signatures, or plaintext encryption.

Shelf life of data sensitivity

Even though quantum computers are currently only capable of breaking algorithms that are known to be relatively weak, and new quantum-resistant algorithm standards are not yet fully defined, your data sensitivity timeline likely overlaps with that of cryptanalytical-capable quantum computers.

For example, state secrets, intellectual property, customer information, or investor relations must be kept secret for decades or longer to protect an organization's competitive edge and avoid the risks of future legal liabilities, embarrassments, or boycotts.

Advanced adversaries, such as foreign states and criminal proxies, already steal encrypted data with the intent to decrypt it once practical attacks become available under the "Harvest now, decrypt later" approach. Time is a risk factor that cannot be mitigated; organizations must act now.

Get quantum-ready with Fortanix

Fortanix helps contain future data exposure risks and provides solutions for all critical steps in your post-quantum readiness journey. The first phase is to discover your cryptographic security posture. Fortanix Key Insight discovers all encryption keys and data services in the cloud to assess and track your cryptographic security posture. It reveals where all encryption keys are, and how they are used by data services across multicloud environments.

Cryptographic agility is essential for organizations to transition to a strong and resilient crypto posture. Fortanix provides a suite of solutions to give back the visibility and control of an organization's cryptographic operations across multiple clouds, classical datacenters, and individual regions. Organizations can transition smoothly to new cryptographic standards with an efficient use of resources. With Fortanix, organizations can consolidate data security and achieve crypto agility through three key steps:

Discover

Gain complete and centralized visibility into where keys are and how data services use them. An exact inventory of your cryptographic security posture is fundamental to an effective and resilient security strategy.

Assess

Identify how well your data is protected against a quantum attack. With an intuitive dashboard, Fortanix helps identify and prioritize where and when to apply new quantum-resistant algorithms.

Remediate

Take back control of your keys: centrally manage their lifecycles and govern consistent policies across hybrid multicloud. Crypto-agility is essential to a fast and smooth transition to quantum-proof algorithms.

Use Cases



Data at Rest Encryption

Encrypt sensitive data stored on servers and cloud storage with PQC algorithms.



Secure Communications

Secure network communications like HTTPS or VPN with PQC-protected confidentiality.




Digital Signing

Sign documents, software, and certificates with PQC algorithms to ensure authenticity and prevent supply-chain attacks.

Supported post-quantum algorithms :

Fortanix already supports most of the quantum-resistant Commercial National Security Algorithm Suite 2.0 algorithms and is ready to adopt pending NIST standards once they become available.

	Algorithm	NIST Standard Name	Usage
 CNSA 2.0	Leighton-Micali Signature (LMS)*		Signatures
	Advanced Encryption Standard (AES)		Encryption
	Secure Hash Algorithm (SHA)		Signatures
	CRYSTALS-Kyber*	ML-KEM	Encryption and key exchange
	Xtended Merkle Signature Scheme (XMSS)*		Signatures
	CRYSTALS-Dilithium	ML-DSA	Signatures
	SPHINCS+	SLH-DSA	Signatures
	Falcon	NL-DSA	Signatures
	McEliece		Encryption and key exchange
		supported	roadmap 2024

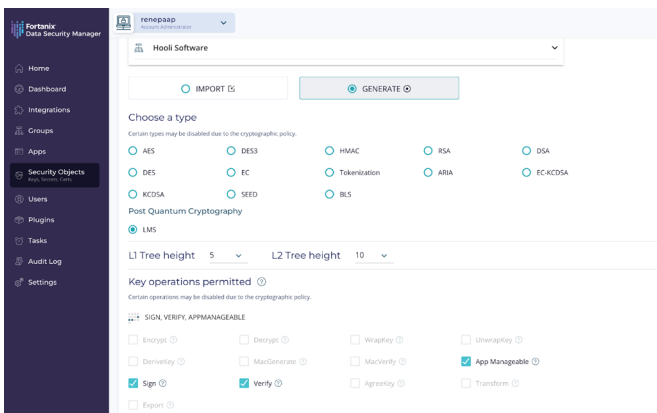
Benefits and features

Consolidated control and agility

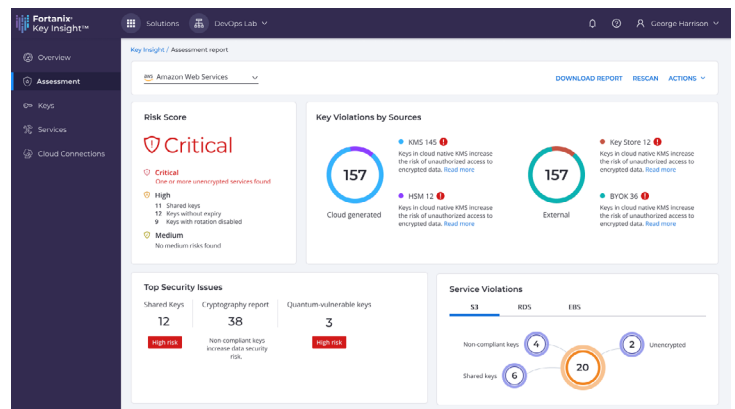
- Fortanix helps eliminate operational complexity for security, data, and developer teams, enabling them to adopt post-quantum algorithms rapidly. The unified platform enables use cases for Enterprise Key Management, Data Masking and Tokenization, and Secure DevOps across hybrid multicloud environments.
- The Fortanix platform provides centralized, scalable key management and the ability to prepare your HSM infrastructure for the post-quantum era by gradually transitioning to integrated HSMs for the most secure key storage (FIPS 140-2 Level 3).

About Us

Fortanix is a global leader in data security. We prioritize data exposure management, as traditional perimeter-defense measures leave your data vulnerable to malicious threats in hybrid multicloud environments. Our unified data security platform makes it simple to discover, assess, and remediate data exposure risks, whether it's to enable a Zero Trust enterprise or to prepare for the post-quantum computing era. We empower enterprises worldwide to maintain the privacy and compliance of their most sensitive and regulated data, wherever it may be. For more information, visit <https://www.fortanix.com>.



Create quantum-resistant keys



Discover quantum-vulnerabilities