SOLUTION BRIEF

Fortanix

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. By using specific algorithms, quantum computers will be able to reconstruct the cryptographic key pairs that secure your sensitive data.

While current encryption algorithms can increase quantum resistance by significantly increasing the key length, this approach requires significant increases in computing capacity and only delays the inevitable—quantum computing will catch up.

Shelf life of data sensitivity and encryption strength

An organization's security strategy must determine the appropriate security level for data of different purposes and classifications. One important thing to consider is how long the data must remain confidential. For example, government agencies have strict rules about levels of classified information and how long it should stay locked up to avoid harming national security or international relations. Any modern organization has strictly defined regulatory obligations to protect regulated data such as healthcare records (HIPAA) or payment data (PCI DSS). Intellectual property (IP) and supply chain details should also remain private to protect an organization's competitive edge and avoid the risks of future legal liabilities, embarrassment, and boycotts.

Even if confidential data is protected by today's top cryptographic algorithms, quantum computers will be able to help reveal this data. Increasing the cryptographic key length increases the encryption strength but only buys limited time against the rapid, exponential advancements in quantum computing. 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. The quantum computing-aided cryptanalysis threat is not imminent; it is immediate. Organizations must act now.

Fortanix Post Quantum Cryptography Solution

The unified Fortanix data security platform makes it easy for organizations to transition to new cryptographic standards without disrupting operations. Fortanix enables organizations to centralize and gain complete control of their cryptographic operations across multiple clouds, classical datacenters, and individual regions. With Fortanix, organizations can consolidate data security and achieve crypto agility through three key steps:

info@fortanix.com | 3910 Freedom Circle Suite 104, Santa Clara, CA 95054, United States

Discover

With a centralized solution, organizations gain complete visibility into what keys are in use and how human or machine identities use them. A thorough inventory of how your sensitive data is used and protected is fundamental to anysecurity strategy.

Assess

Identify how well your data is protected and how it aligns with current security policies. With an intuitive dashboard, Fortanix helps identify and prioritize where and when to apply new quantum-proof algorithms.

Remediate

Fortanix enables organizations to own and control the lifecycle of all encryption keys. Crypto-agility accelerates the deployment of quantum-proof algorithm standards. Fortanix supports the latest NSA-recommended quantum-resistant algorithms and rapidly implements the latest NIST standards into its SaaS platform.

Supported post-quantum algorithms :

Commercial National Security Algorithm Suite 2.0 (CNSA 2.0)

Algorithm	Type
Leighton-Micali Signature (LMS)	Asymmetric algorithm for digitally signing firmware and software
Xtended Merkle Signature Scheme (XMSS)*	Asymmetric algorithm for digitally signing firmware and software
Advanced Encryption Standard (AES) 256-bit	Symmetric block cipher for information protection
Secure Hash Algorithm (SHA) 384 or 512 bit	Algorithm for computing a condensed representation of information
CRYSTALS-Kyber**	Asymmetric algorithm for key exchange
CRYSTALS-Dilithium*	Asymmetric algorithm for digital signatures

* Roadmap
** Experimental support

info@fortanix.com | 3910 Freedom Circle Suite 104, Santa Clara, CA 95054, United States

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).

Harden Zero Trust strategy

- Take full key custody for cloud projects with External Key Management for Google External Key Manager (EKM) or AWS KMS External Key Store (XKS).
- Control the use of keys in the cloud with Bring Your Own Key (BYOK) and/or Bring Your Own Key Management System (BYOKMS) functionality.
- Enforce least-privilege data access with Role-Based Access Control (RBAC), quorum controls, and immutable logging of all crypto operations.

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.