Fortanix

Post-Quantum Readiness

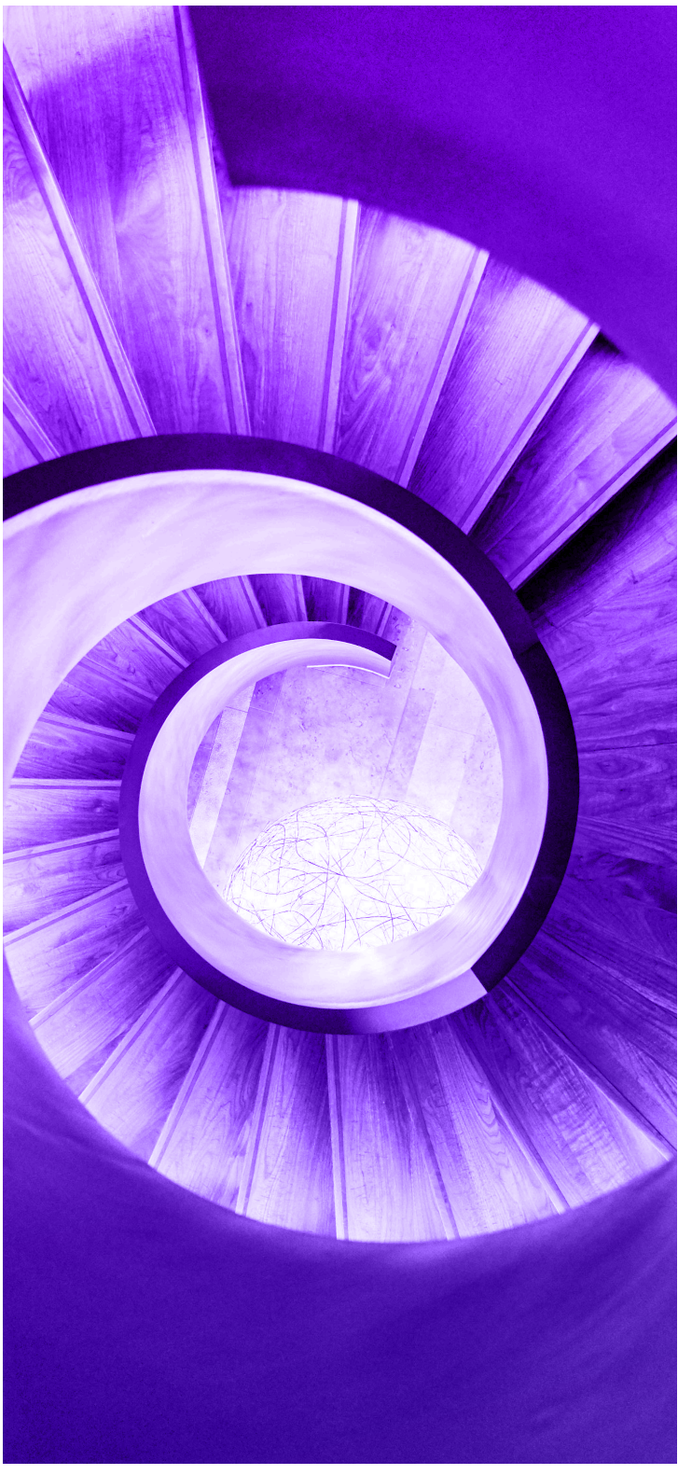
Secure Your Data Now from the Inevitable Quantum Risks – Before it's Too Late

Data is the lifeblood of every organization, yet it has never been more vulnerable. While advances in cryptography, key encryption, and management have created a false sense of security, the reality is that shifting network boundaries, hybrid on-premises and multicloud environments, and fragmented data ownership have made traditional, typically manual security approaches ineffective and outdated.

As organizations struggle to manage the rising costs and complexity of data security, advances in quantum computing will render current protections obsolete. Within five years, quantum computers will be able to break most widely used public key cryptographic algorithms, putting long-term sensitive data at risk. Any data that will retain value beyond five years—customer information, PII, employee records, proprietary company and product details, and even assets you haven't identified—remains vulnerable. For example, encrypted data is being stolen today with the intent to decrypt it in the future, once quantum computing is available.

Governments and private organizations are already taking proactive steps to prepare for the impending threat. Quantum-resistant encryption algorithms are available today, and NIST recently released new standards for key exchange, digital signatures, and plaintext encryption to strengthen data security in the post-quantum era.

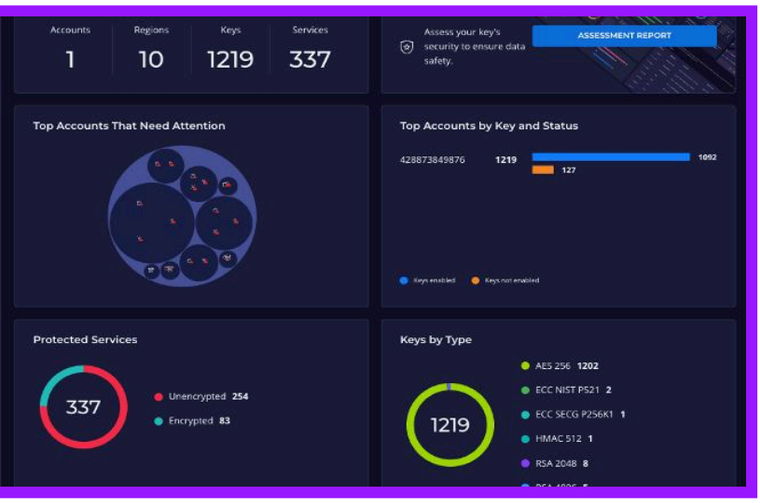
If your organization hasn't started executing a Post-Quantum Computing Readiness Plan, now is the time. And if you have started, implementing the Fortanix platform can help streamline operations, accelerate readiness, and reduce both risk and cost.



Fortanix gets you quantum-ready

Fortanix continuously monitors and adapts as new PQC algorithms become available to stay ahead of evolving risks. The Fortanix platform is designed to support you through all phases of the Post-Quantum Readiness process whether you are dealing with data at rest, in transit, or in use.

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



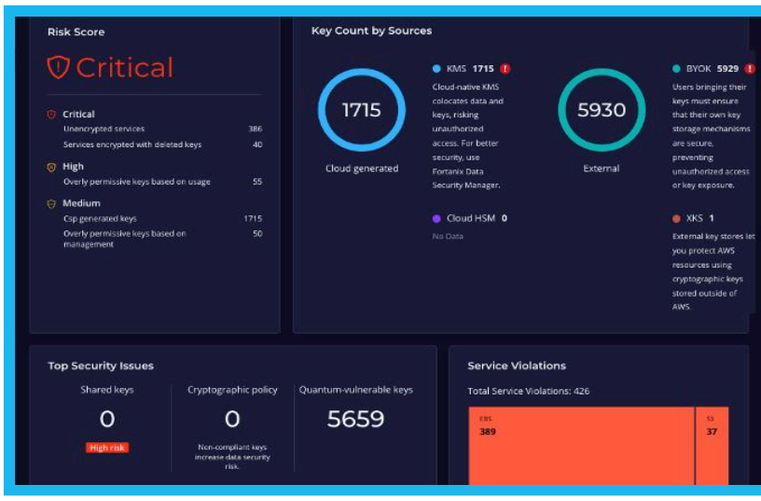
Key Insight discovery view

DISCOVER

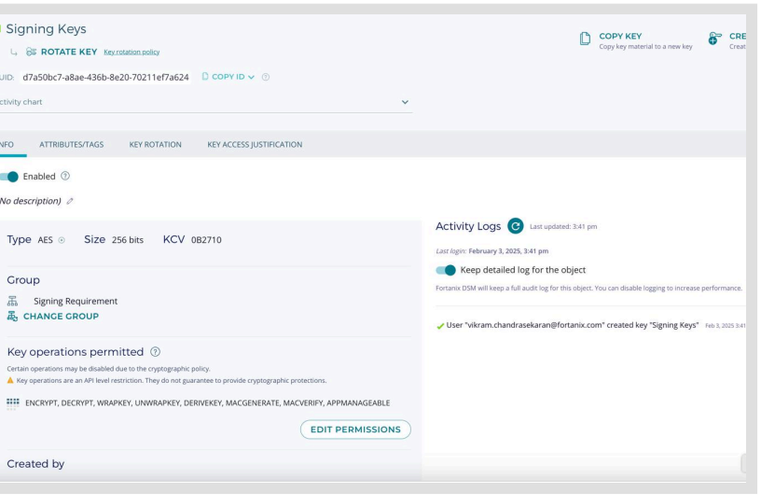
- Maps your organization's entire cryptographic security posture
- Inventories all encryption keys and data services across multi-cloud, multi-geography and on-premise environments
- Provides complete visibility into key locations, statuses, and usage across critical data services

PQC ASSESSMENT

- Benchmarks your organization's cryptographic security posture against emerging post-quantum computing threats
- Identifies gaps in security posture and detects data services lacking proper encryption or protection
- Prioritizes vulnerabilities through an intuitive dashboard and heat maps



Key Insight assessment view



Rotate to AES-256 key in DSM

PQC TRANSITION

- Centrally manage all encryption keys and policies
- Ensures compliance and governance with the latest security standards, algorithms and policies.
- Automates manual processes to eliminate human error, reduce inconsistencies, and enhance overall data security

CRYPTO-AGILITY

With processes and tools in place, organizations now have an agile framework for quickly adapting to new cryptographic systems. PQC Readiness is a continuous process, as enterprises have a hyper-dynamic infrastructure where new services and systems launch regularly, potentially disrupting the cryptographic security footprint.

Supported Post-Quantum Algorithms

Fortanix supports the full suite algorithms in the Commercial National Security Algorithm Suite (CNSA) 2.0. Our platform is built for agility and will swiftly implement updates and new standards when they arise.

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher for information protection	FIPS PUB 197	Use 256-bit keys for all classification levels.
CRYSTALS-Kyber (ML-KEM)	Asymmetric algorithm for key establishment	FIPS PUB 203	Use Level V parameters for all classification levels.
CRYSTALS-Dilithium (ML-DSA)	Asymmetric algorithm for digital signatures	FIPS PUB 204	Use Level V parameters for all classification levels.
Secure Hash Algorithm (SHA)	Secure Hash Algorithm (SHA)	FIPS PUB 180-4	Use SHA-384 or SHA512 for all classification levels.
Leighton-Micali Signature (LMS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels. SHA-256/192 recommended.
Xtended Merkle Signature Scheme (XMSS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels.

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