



ENTERPRISE SECURITY BRIEF

Why Enterprises Should Buy the Purism PQC Encryptor

A practical path to high-performance, post-quantum network encryption

SANTA ROSA SOFTWARE

Chattanooga, TN • Washington, DC

santarosasoftware.com



Executive Summary

The **Librem PQC Encryptor** provides enterprises with an immediate, deployable solution for protecting **data-in-transit** against both current cyber threats and future quantum-computing attacks. Unlike traditional network encryption products that rely on RSA and ECC algorithms vulnerable to future quantum computers, the PQC Encryptor is built around the latest **NIST-standardized post-quantum cryptography (PQC)** and offers a drop-in architecture that helps organizations align with emerging U.S. government mandates and guidance. [\[csrc.nist.gov\]](https://csrc.nist.gov)

The Market Reality: Quantum Risk Is No Longer Theoretical

The biggest cybersecurity challenge associated with quantum computing is the "Harvest Now, Decrypt Later" threat. Adversaries can capture encrypted network traffic today and retain it until cryptographically relevant quantum computers become available, at which time traditional public-key cryptography could be broken. U.S. government agencies have formally recognized this risk and directed organizations to begin migration planning now. [\[whitehouse.gov\]](https://whitehouse.gov), [\[whitehouse.gov\]](https://whitehouse.gov)

For enterprises handling intellectual property, government contracts, financial transactions, healthcare records, critical infrastructure data, long-lived confidential information waiting for quantum computers to arrive is already too late. [\[whitehouse.gov\]](https://whitehouse.gov), [\[whitehouse.gov\]](https://whitehouse.gov), [\[media.defense.gov\]](https://media.defense.gov)



Built on NIST-Approved Post-Quantum Standards

One of the strongest selling points of the PQC Encryptor is that it uses **NIST FIPS 203**, the first official U.S. federal post-quantum cryptography standard, published in August 2024. [\[csrc.nist.gov\]](https://csrc.nist.gov), [\[nist.gov\]](https://nist.gov)

Specifically:

- Uses **ML-KEM (Module-Lattice Key Encapsulation Mechanism)**, derived from CRYSTALS-Kyber.
- ML-KEM is standardized in **FIPS 203**.
- NIST identifies ML-KEM as secure against both classical and quantum adversaries.
- ML-KEM is the new federal standard for quantum-resistant key establishment. [\[csrc.nist.gov\]](https://csrc.nist.gov), [\[nist.gov\]](https://nist.gov), [\[nist.gov\]](https://nist.gov)

For enterprise buyers, this means they are not investing in experimental technology. They are investing in a solution aligned with the cryptographic standards selected by the U.S. government after nearly a decade of evaluation. [\[nist.gov\]](https://nist.gov), [\[csrc.nist.gov\]](https://csrc.nist.gov)

Alignment with NSA Quantum Security Guidance

The National Security Agency has repeatedly warned organizations to prepare for the transition to quantum-resistant cryptography and has established the **Commercial National Security Algorithm Suite (CNSA) 2.0** as the roadmap for National Security Systems. [\[media.defense.gov\]](https://media.defense.gov), [\[media.defense.gov\]](https://media.defense.gov), [\[nsa.gov\]](https://nsa.gov)

NSA guidance emphasizes:

- Planning and budgeting for quantum-resistant cryptography now.
- Replacing vulnerable public-key algorithms.
- Moving toward NIST-approved post-quantum algorithms.
- Preparing systems for future compliance requirements. [\[media.defense.gov\]](https://media.defense.gov), [\[nsa.gov\]](https://nsa.gov)



The Encryptor's use of NIST-standardized PQC directly supports organizations looking to align with this strategic direction. [\[csrc.nist.gov\]](https://csrc.nist.gov)

Supports Federal and Defense Supply Chain Readiness

Federal agencies and contractors are increasingly being required to establish plans for migration to PQC.

Examples include:

White House National Security Memorandum 10 (NSM-10)

NSM-10 directs the federal government to begin mitigating the risks posed by quantum computers and transition toward quantum-resistant cryptography. [\[whitehouse.gov\]](https://www.whitehouse.gov), [\[whitehouse.gov\]](https://www.whitehouse.gov)

OMB Memorandum M-23-02

The Office of Management and Budget directed federal agencies to inventory cryptographic systems and begin preparing for PQC migration, specifically warning about the "harvest now, decrypt later" threat. [\[whitehouse.gov\]](https://www.whitehouse.gov)

OMB Memorandum M-26-15

OMB now requires agencies to execute a prioritized migration strategy and develop formal PQC migration plans, with implementation milestones extending through 2035. [\[whitehouse.gov\]](https://www.whitehouse.gov), [\[federalnew...etwork.com\]](https://federalnewsnetwork.com)

NSA CNSA 2.0

The NSA has established post-quantum requirements for National Security Systems and continues to push adoption of quantum-resistant cryptography across defense ecosystems. [\[media.defense.gov\]](https://media.defense.gov), [\[nsa.gov\]](https://nsa.gov), [\[media.defense.gov\]](https://media.defense.gov)

Bottom line: Organizations selling into the U.S. federal government, Department of Defense, intelligence community, or critical infrastructure sectors can demonstrate proactive PQC readiness today by deploying the PQC Encryptor. [\[whitehouse.gov\]](https://www.whitehouse.gov), [\[media.defense.gov\]](https://media.defense.gov)



Drop-In Deployment with Minimal Network Disruption

Unlike many PQC initiatives that require extensive application redesign, the PQC Encryptor is deployed as an appliance pair.

Benefits include:

- Drop-in deployment
- Works across existing network environments
- No application rewrites
- No major infrastructure overhaul
- Quantum-safe protection for entire network links

Two encryptors are deployed at opposite ends of a connection, encrypting all traffic between locations.

For enterprises, this translates into faster adoption, lower risk, and accelerated time-to-value.

Enterprise-Class Performance

The PQC Encryptor comes in multiple deployment options:

Model	Throughput
PQC Encryptor 10	10 Gbps
PQC Encryptor 100	100 Gbps
PQC Encryptor 400	400 Gbps

The solutions are designed for line-rate operation while maintaining post-quantum protection.



This allows organizations to deploy PQC protection across:

- Data centers
- Government networks
- Defense facilities
- Critical infrastructure
- Financial trading environments
- Healthcare systems

without sacrificing throughput.

Unique Key Protection Architecture

The PQC Encryptor emphasizes a differentiator that resonates strongly with security-sensitive organizations:

The secret keys generated on the device never leave the device.

Benefits include:

- Reduced key exposure risk
- Minimized insider threat vectors
- Stronger cryptographic custody controls
- Simplified security governance

Administrators can manage devices and certificates without accessing the secret keys themselves.



Ideal Messaging for Enterprise Buyers

Future-Proof Security

Protect sensitive communications from both current attackers and future quantum adversaries. [\[whitehouse.gov\]](#), [\[whitehouse.gov\]](#)

Government-Aligned Cryptography

Built on NIST FIPS 203 standards and aligned with emerging NSA and federal quantum security strategies. [\[media.defense.gov\]](#)

Compliance Readiness

Prepare for evolving federal, defense, and critical infrastructure requirements before mandates become urgent. [\[whitehouse.gov\]](#), [\[whitehouse.gov\]](#), [\[media.defense.gov\]](#)

Operational Simplicity

Deploy quantum-safe encryption without redesigning applications or rebuilding networks.

High-Speed Protection

Scale from 10 Gbps to 400 Gbps while maintaining quantum-resistant encryption.

Executive Positioning Statement

The Purism PQC Encryptor enables organizations to move from quantum-risk awareness to quantum-risk mitigation today. Built on NIST FIPS 203 post-quantum cryptography, aligned with NSA and federal migration strategies, and engineered as a high-performance drop-in network encryption solution, the PQC Encryptor gives enterprises a practical path to protecting critical data against both present-day threats and the coming quantum era.

For more information on the PQC Encryptor, please visit <https://santarosasoftware.com/pqc-encryptor>.