

Upgrade to next-generation security for the quantum era

What's the offer?

CNSA 2.0 mandates that all new national security systems (NSS) acquisitions be quantum proof, starting Jan 1, 2027.

With NIST-standardized algorithms like ML-KEM and ML-DSA, and the rising threat of Harvest-Now, Decrypt Later (HNDL) attacks, the risk is immediate. The challenge is executing the transition fast, without disrupting operations.

EigenQ and HPE solve this with a PQC+™ security bundle built on HPE ProLiant Compute and EigenQ's hardware-rooted trust stack. Unlike software-only approaches, this pre-integrated platform delivers next-generation security from silicon to application, using NIST-approved PQC algorithms alongside hardware-rooted trust, quantum entropy, and crypto agility.

The result: Easy CNSA 2.0 compliance, reduced migration complexity, and deployment in weeks, not years, with no "rip & replace."

Who will buy it?

Target industries and use cases:

- **Federal/Defense:** Compliance with federal PQC mandates, high-assurance server refresh, national security systems and high-value asset (HVA) modernization, quantum-ready infrastructure for agencies and primary contractors, deployments aligned with secure supply chain requirements
- **Critical infrastructure and public sector organizations:** Trusted servers and appliances for utilities, transportation, public safety, state/local environments that need stronger integrity controls and cryptographic modernization
- **Financial services and regulated enterprises:** Quantum-ready private cloud, certificate authority and key-service nodes, trusted compute infrastructure that delivers attestation, secure boot, and stronger entropy
- **Managed service providers, everything-as-a service (XaaS) providers, and other service providers:** Repeatable HPE-based secure service offerings, PQC-hardened cloud nodes, managed trust services that can be packaged rather than custom-built each time
- **Healthcare:** PQC-hardened infrastructure for regulated care delivery environments, high-value application servers, secure private cloud nodes, future-proofed cryptographic services

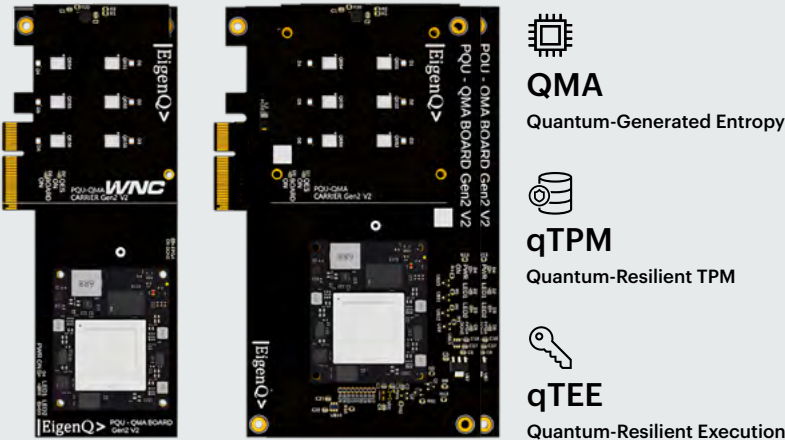
Business value

- CNSA 2.0 & NIST readiness, today
- Reduces PQC migration complexity
- Avoids fragmented software-only approaches
- Accelerates time to quantum readiness
- Provides a repeatable, standardized HPE-based platform
- Delivers hardware-rooted trust, attestation, and cryptographic agility
- Quantum-resilience systems, from silicon to application
- Reinforces supply chain assurance and integration credibility

EigenQ's PQC+™ technology can be integrated into existing infrastructure, in weeks not years,

no "rip & replace".

EigenQ PQC+ bundle



HPE ProLiant servers running on Intel® Xeon® processors



Customer pain points and solution benefits

Pain point	Solution benefit
By January 1, 2027, all new national security systems must comply with CNSA 2.0	HPE and EigenQ’s solution directly addresses the CNSA 2.0 mandate by making compliance achievable without redesigning your entire infrastructure
Software-only PQC migration is incomplete and quantum vulnerable	Provides a bounded, integrated path that combines server platform, PQC software, quantum random number generator (QRNG) entropy, secure boot, attestation, and trust controls in one offering
Customers need stronger hardware-rooted trust, not just algorithm support	Includes quantum-generated entropy, attestation anchored in a Trusted Platform Module (TPM), secure firmware validation, and integrity enforcement to strengthen the platform trust model
Federal and regulated buyers need a clearer compliance, sourcing, and integration story	Strengthens the federal narrative by using an HPE-integrated delivery model and a more credible secure-supply-chain story
Partners need solutions that work in real infrastructure and are easier to explain and deploy	Aligns to HPE ProLiant Compute infrastructure, Intel Xeon processor-based platform motions, modern API-driven manageability, and channel-ready packaging
Customers do not want narrowly focused solutions; they want a repeatable but flexible architecture	Can be positioned as a secure server or appliance, a private cloud node, or as part of a future HPE Morpheus-managed trusted architecture, enabling more strategic infrastructure discussions
U.S. federal cybersecurity policy requires ready-to-deploy PQC solutions. No internal integration	Solution-in-a box: Fully validated solutions. Right-sized configurations to fit any deployment

Unpredictable pricing models and the need to manage time-consuming, complex procurement processes	Ready-to-quote same day with competitive prices
---	---

Solution components

- **EigenQ’s PQC+ bundle** goes far beyond a software-only PQC layer on a standard server (which will not be CNSA 2.0 compliant). Components include quantum entropy management (QEM) software, the EigenQ Quantum Random Number Generation Massive Acceleration (QMA) PCIe quantum entropy module; a quantum Trusted Platform Module (qTPM) root of trust, and secure boot and firmware integrity controls.
- **The HPE ProLiant Compute platform** (such as the DL360 or DL380) lays a solid execution foundation for the PQC+™ bundle, improving federal readiness, supply-chain positioning, and deployment credibility. The solution is designed to align to the standards-based manageability and hardware visibility expected in enterprise HPE environments.
- **Intel Xeon processor-based infrastructure** supports confidential computing through Intel® Trust Domain Extensions (Intel® TDX), Intel® Software Guard Extensions (Intel® SGX), and trusted workload execution concepts that emphasize hardware-rooted trust and attestation.
- **This is a foundational upgrade to modern, next-generation security architecture.**

More resources

- [EigenQ website](#)
- [HPE ProLiant Compute](#)
- [What is Post-Quantum Cryptography? article](#)
- [Addressing the Quantum Threat article](#)

© Copyright 2026 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Intel and Intel Xeon are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries. All third-party marks are property of their respective owners.

a00159324enw

Visit HPE.com

HEWLETT PACKARD ENTERPRISE
hpe.com