

4 key steps to prepare for post-quantum cryptography

Advancements in quantum computing are expected to break many of today's widely used public-key encryption methods over the coming decade. U.S. federal agencies are now required to submit post-quantum cryptography (PQC) migration plans by late October 2026, with prioritized migration by 2030 and full migration by 2035.¹ For some organizations in regulated industries and the public sector, new PQC requirements are already shaping security roadmaps and procurement decisions through as early as 2027.² At the same time, "harvest now, decrypt later" attacks are a present concern: Adversaries can capture encrypted data today and decrypt it once quantum-capable systems emerge. To address both the long-term cryptographic transition and today's exposure, consider these 4 key steps to prepare for PQC.

1 Assess sensitive data and existing cryptographic protocols

To begin preparing for PQC, organizations must assess the current vulnerability of the data they need to safeguard. They must bring together a multifaceted team (including representatives from business operations, legal and compliance, IT, and other relevant departments) to identify and trace all access paths to that data. They can use these findings to classify what data is or will be considered sensitive now, in the near future, and in the distant future, among other considerations. Next, organizations need to take inventory of the cryptographic protocols currently in place and assess which are in most urgent need of updating, which can be modified, and which must remain the same due to hardware or software limitations.

2 Identify which assets need to be prioritized

Once teams have a clear understanding of their organization's sensitive data, they can prioritize which assets they need to safeguard right away. It is not practical, or even realistic, to address the security of all assets at once. It is crucial to take a pragmatic approach to planning—drawing on the insights gained from preliminary work—to carefully consider which assets and systems should be prioritized and which can be addressed at a later date.

3 Test new quantum-resistant algorithms in the organization's environment

Most compliance entities recommend migrating to new PQC protocols and algorithms, including the standards the National Institute of Standards and Technology (NIST) finalized in August 2024, as soon as possible.³ The sooner teams begin testing algorithms and addressing issues that could prevent a successful transition, the more prepared an organization will be for what will soon be mandatory compliance requirements. This will also help mitigate risk from "harvest now, decrypt later" attacks. To begin testing quantum-resistant cryptography, organizations should adopt or upgrade to Red Hat® Enterprise Linux® 10.2, which delivers NIST-approved algorithms, including Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) for key exchange and Module-Lattice-Based Digital Signature Algorithm (ML-DSA) for signing across Transport Layer Security (TLS), Secure Shell (SSH), and software supply chain verification, with hybrid package signatures and expanded Federal Information Processing Standards (FIPS)-compatible SSH support in the latest release.

1 Office of Management and Budget. Execution of the Migration to Post-Quantum Cryptography, Memorandum M-26-15, 24 June 2026.

2 Ivezić, Marin. "France's ANSSI Will Block PQC-Free Products From Certification Starting 2027." PostQuantum.com, 17 June 2026.

3 "NIST Releases First 3 Finalized Post-Quantum Encryption Standards." National Institute of Standards and Technology, 13 Aug. 2024.

4 Start the full transition and move into production

Implementing new quantum-resistant algorithms is the final and most complex part of the process. Rather than a quick sprint to immediate results, organizations need to approach this step as a sustained effort with long-term benefits as the goal. Updating

every cryptographic algorithm throughout an environment will not happen immediately, but the insights gained and priorities identified in the preliminary steps will set organizations up for sustainable success. As they apply changes to cryptographic protocols and incorporate quantum-resistant algorithms in production, they must pay special attention to any interdependencies identified during the testing phase in order to mitigate unintended consequences or downtime.

Start preparing for post-quantum cryptography today

Explore how [Red Hat Enterprise Linux 10](#) incorporates quantum-resistant algorithms that can help organizations prepare for the era of PQC.



About Red Hat

Red Hat helps customers standardize across environments, develop cloud-native applications, and integrate, automate, secure, and manage complex environments with [award-winning](#) support, training, and consulting services.

f facebook.com/redhat
x x.com/RedHat
in linkedin.com/company/red-hat

redhat.com
#4922618_0926

North America	Europe, Middle East, and Africa	Asia Pacific	Latin America
1 888 REDHAT1 www.redhat.com	00800 7334 2835 europe@redhat.com	+65 6490 4200 apac@redhat.com	+54 11 4329 7300 info-latam@redhat.com