4 key steps to prepare for post-quantum cryptography

Advancements in quantum computing are expected to make cryptography standards unsafe by as early as 2029.[1] This means encryption resistant to quantum computing-powered decryption will soon be a necessity for every business. To address this looming threat, as well as "harvest now, decrypt later" attacks that are already a present threat, your organization should consider these 4 key steps to prepare for post-quantum cryptography.

1 Assess your organization's sensitive data and existing cryptographic protocols

To begin preparing for post-quantum cryptography, you should assess the current vulnerability of the data your organization needs to safeguard.

This is best done by bringing together a multifaceted team (including representatives from business operations, legal and compliance, IT, and any other relevant departments) to identify and trace all access paths to that data. From these findings, your teams can begin to classify what data is considered sensitive now, in the near future, or in the distant future, among other considerations.

Next, it is important to take inventory of the cryptographic protocols your organization currently has in place, and assess which protocols 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 of your assets need to be prioritized

Now that your teams have a clear understanding of your organization's sensitive data, you can begin to prioritize which assets need to be safeguarded right away.

It is not practical, or even realistic, to address the security of all your various assets all at once. This is why it is crucial to take a pragmatic approach to planning—drawing on the insights gained from the preliminary work your teams have already done—to carefully consider which assets and systems should be a priority to address right away and which can be addressed at a later date.

1 Horvath, Mark. "Begin Transitioning to Post-Quantum Cryptography Now." Gartner, 30 Sept. 2024

3 Begin testing new quantum-resistant algorithms in your environment

Most compliance entities are advising organizations to start migrating to new post-quantum cryptographic protocols and algorithms as soon as possible; including the 1st finalized standards, released in August 2024 by the National Institute of Standards and Technology (NIST).[2]

The sooner your teams can begin testing algorithms and addressing issues that could prevent your organization from successfully transitioning to them, the more prepared you will be for what will soon be mandatory compliance requirements, and the better you can mitigate risk from "harvest now, decrypt later" attacks.

To help your organization get started with testing new quantum-resistant algorithms, consider adopting or upgrading to Red Hat® Enterprise Linux® 10. This operating system (OS) includes the 1st installment of quantum-resistant algorithms—including OpenSSL, ML-KEM (FIPS 203), and ML-DSA (FIPS 204)—that provide key-exchange, encryption, and signing, with added functionality planned for subsequent releases.

4 Commence your full-scale transition and start moving into production

While it is the final step in this process, implementing new quantum-resistant algorithms is the most extensive and complex part of the process.

Rather than a quick sprint to immediate results, your organization needs to approach this step as a sustained effort, with long-term benefits as the goal.

Updating every cryptographic algorithm throughout your environment is not going to happen immediately, but the insights gained and priorities identified in the preliminary steps will set your organization up for sustainable success.

As you begin to apply changes to your cryptographic protocols and incorporate quantum-resistant algorithms in production, special attention will need to be provided to any interdependencies that were identified during the testing phase in order to mitigate unintended consequences or downtime.

Start preparing for post-quantum cryptography today

Explore this page to learn more about how Red Hat Enterprise Linux 10 incorporates quantum-resistant algorithms that can help your organization prepare for the era of post-quantum cryptography.

---

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