# Microsoft enhances Windows 11 with quantum-resistant cryptography to counter emerging cyber threats



Microsoft has announced significant advancements aimed at fortifying Windows 11 against the burgeoning threat posed by quantum-powered cyberattacks. As quantum computers advance from specialized laboratories into commercial applications, the potential risk to existing encryption methods increases dramatically. Experts project that quantum technology could potentially disrupt current cryptographic algorithms, presenting a foundational challenge for cybersecurity. This reality has prompted Microsoft to introduce a range of post-quantum cryptography (PQC) capabilities designed to bolster security measures within both Windows and Linux systems.

The recent updates include the introduction of ML-KEM and ML-DSA algorithms via the Cryptography API: Next Generation (CNG) libraries for Windows Insiders, along with enhancements to the SymCrypt-OpenSSL for Linux. These developments allow developers and organisations to experiment with PQC within their operational environments, laying groundwork for future-proofing against what Microsoft terms "harvest now, decrypt later" attacks. This proactive approach aligns with the National Institute of Standards and Technology's (NIST) standardisation of PQC algorithms, marking a crucial step in the industry's collective effort to transition towards quantum-resistant security measures.

Microsoft’s focus on 'Crypto Agility' is vital in this context. The concept underscores the necessity for systems that can adapt to evolving cryptographic standards. “PQC algorithms are relatively new, and it is prudent not to consider the initial generation of PQC algorithms as the definitive solution but rather view this as an evolving field,” Microsoft stated. This perspective is especially critical given that researchers identify quantum computing as potentially the "biggest security threat of all time." Such recognition of quantum threats has catalysed a wider industry awareness, prompting numerous firms to prioritise the development and adoption of quantum-safe technologies.

For Microsoft, the journey towards a quantum-safe future is not a recent pursuit. Since 2014, the company has been heavily invested in PQC research, collaborating with international standards organisations and driving efforts to assist in the seamless transition to these new cryptographic measures. As a leading member of the Open Quantum Safe project, Microsoft has also worked on establishing relevant industry standards. Their commitment is further evidenced by the introduction of quantum-resistant features in the SymCrypt cryptographic engine, which significantly enhances security protocols against emerging threats.

Windows 11's architecture exhibits a range of built-in security features designed specifically to address contemporary vulnerabilities. These include hardware-based protections like a Trusted Platform Module (TPM), which safeguards cryptographic information with encryption, hypervisor-protected code integrity, and Kernel Direct Memory Access (DMA) protection. In combination with the latest PQC updates, these measures represent a comprehensive strategy to enhance the operating system's integrity and safeguard it from both current and future threats.

The quantum computing landscape is rapidly evolving, and as Microsoft continues to upgrade its security apparatus, the urgency to protect sensitive information has never been greater. The involvement of companies like Microsoft in developing quantum-safe technology signals a crucial pivot towards a more resilient cybersecurity framework, essential for protecting data in an era where the capabilities of quantum computing could redefine the security landscape.

## Reference Map:

* Paragraph 1 – [[1]](https://www.techradar.com/pro/security/windows-11-is-getting-top-level-protection-against-the-next-generation-of-quantum-cyberattacks), [[4]](https://arstechnica.com/security/2024/09/microsoft-adds-quantum-resistant-algorithms-to-its-core-crypto-library/)
* Paragraph 2 – [[1]](https://www.techradar.com/pro/security/windows-11-is-getting-top-level-protection-against-the-next-generation-of-quantum-cyberattacks), [[2]](https://blogs.microsoft.com/blog/2023/05/31/building-a-quantum-safe-future/), [[3]](https://techcommunity.microsoft.com/blog/microsoft-security-blog/microsofts-quantum-resistant-cryptography-is-here/4238780)
* Paragraph 3 – [[2]](https://blogs.microsoft.com/blog/2023/05/31/building-a-quantum-safe-future/), [[6]](https://cybermagazine.com/articles/microsoft-warns-about-quantum-computing-cyber-threats)
* Paragraph 4 – [[5]](https://www.starwindsoftware.com/blog/windows-11-security-features-in-2024/), [[6]](https://cybermagazine.com/articles/microsoft-warns-about-quantum-computing-cyber-threats)
* Paragraph 5 – [[1]](https://www.techradar.com/pro/security/windows-11-is-getting-top-level-protection-against-the-next-generation-of-quantum-cyberattacks), [[7]](https://www.csoonline.com/article/2121652/microsoft-amps-up-focus-on-windows-11-security-to-address-evolving-cyberthreats.html)

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.techradar.com/pro/security/windows-11-is-getting-top-level-protection-against-the-next-generation-of-quantum-cyberattacks> - Please view link - unable to able to access data
2. <https://blogs.microsoft.com/blog/2023/05/31/building-a-quantum-safe-future/> - Microsoft has been investing in post-quantum cryptography (PQC) research and development since 2014, collaborating with international standards bodies and supporting the National Institute of Standards and Technology (NIST) in their efforts to prepare organizations for the PQC transition. The company is a core member of the Open Quantum Safe (OQS) project and leads the PQC working group for SAFECode, aiming to advance industry standards and assist organizations in adopting quantum-safe measures. Microsoft emphasizes the importance of 'Crypto Agility' to ensure solutions remain resilient to evolving PQC standards.
3. <https://techcommunity.microsoft.com/blog/microsoft-security-blog/microsofts-quantum-resistant-cryptography-is-here/4238780> - Microsoft has added support for post-quantum algorithms to its SymCrypt cryptographic engine, marking a significant step towards a quantum-safe future. This addition enables customers to experiment with PQC within their operational environments. The transition to PQC is complex and iterative, requiring organizations to create an inventory of cryptographic assets and develop a risk-based plan for adoption. Microsoft is committed to assisting customers and partners in navigating this transition and optimizing security in the quantum era.
4. <https://arstechnica.com/security/2024/09/microsoft-adds-quantum-resistant-algorithms-to-its-core-crypto-library/> - Microsoft has integrated post-quantum algorithms into its SymCrypt cryptographic library, enhancing the security of Windows 11 against potential quantum-powered cyberattacks. The new algorithm, ML-KEM, is based on lattice-based cryptography, offering resilience against quantum attacks. This development aligns with NIST's standardization of post-quantum algorithms and represents a proactive approach to future-proofing cryptographic systems against emerging quantum threats.
5. <https://www.starwindsoftware.com/blog/windows-11-security-features-in-2024/> - Windows 11 has been built with hardware-based security features, including the requirement of a Trusted Platform Module (TPM) device, which secures cryptographic information with encryption. The operating system also supports hardware-enforced stack protection, Kernel Direct Memory Access (DMA) Protection, and hypervisor-protected code integrity (HVCI). Additionally, Windows 11 introduces Secured-core PCs, which verify a clean and trusted state during startup, and Trusted Boot, which ensures the integrity of the boot process to prevent rootkits and malware from infiltrating the system.
6. <https://cybermagazine.com/articles/microsoft-warns-about-quantum-computing-cyber-threats> - Microsoft has been investing in quantum-safe technologies, including CodeQL, a software tool for analyzing program code, and the Crypto Experience for Azure Quantum Resource Estimator, which assesses the security of public keys. The company warns that quantum computing could potentially break traditional encryption methods, making it crucial to protect data now to ensure a quantum-safe future. Microsoft emphasizes the importance of transitioning to quantum-resistant algorithms to safeguard sensitive information against future quantum threats.
7. <https://www.csoonline.com/article/2121652/microsoft-amps-up-focus-on-windows-11-security-to-address-evolving-cyberthreats.html> - Microsoft has introduced Copilot+ PCs, which are secure-cored and provide firmware protection and dynamic root-of-trust measurement. These PCs feature the Microsoft Pluton security processor, enabled by default, and Windows Hello Enhanced Sign-in Security, which uses specialized hardware and software to protect authentication data. This initiative aims to bolster Windows 11's security against evolving cyber threats, including AI-enabled attacks, by integrating advanced hardware and software protections.