SOLUTION BRIEF

Protect Against Quantum Threats Today and Tomorrow with Fortinet

Executive Summary

The anticipated speed and power of quantum computers are expected to revolutionize what people and businesses can achieve with compute. But the giant leap in capability also comes with a giant threat to cybersecurity. Algorithms that we have counted on for years to keep data secure, such as RSA and Diffie-Hellman, could be broken thanks to the advances that quantum computing brings.

Protecting confidential data is of the utmost importance, and steps need to be taken now to secure it in the future. Fortinet offers a suite of security solutions that can assist in planning and implementing a quantum-safe environment. From understanding the current state of encryption cyphers used in traffic in motion, to support for Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC), Fortinet offers crypto-agility and the ability to move from an unknown state today, to a quantum-secure state in the future.

In 2025, the quantum computing industry hit an inflection point, [...] As a result, the path to quantum utility and the timeline to quantum risk have accelerated. Multiple analyses now place Q-Day (the point a quantum computer may break mainstream public-key crypto) around 2030.[1]

Quantum-Safe Protection Can't Wait

Recent advances in quantum hardware, software, and error correction have significantly shortened projected timelines.

Current estimates for the potential arrival of cryptography-relevant quantum computers (CRQCs) now range from 2029 to 2035. This is well within the lifespan of today's systems and data. While Q-Day is still firmly in the future, vulnerability to quantum computing is a problem that organizations need to address now. Threat actors are collecting data today, with the plan to decrypt this information later when faster processing is available known as "harvest-now decrypt-later" (HNDL) attacks.

Organizations that store or processes information that has a sensitivity life longer than the anticipated gap between now and Q-Day should be cognizant of this risk. This is particularly critical for financial, healthcare, defense, and government institutions, but affects any industry that handles data requiring protection for five to seven years. And, as each year goes by, the runway to Q-Day shortens, which brings more data into danger. Whether Q-Day is three, five, or even 10 years away, the time to act is now.

Quantum-Safe Technologies

When looking at how to move to cryptography that is ready for the quantum world, there are two main technologies: QKD and PQC.

QKD enables two parties to securely exchange cryptographic keys. QKD leverages the principles of quantum physics to detect any eavesdropping and hacking attempts. In QKD, cryptographic keys are generated by an external QKD device and shared with endpoints of a secure tunnel via a defined interface. QKD offers a fully resistant solution to attacks leveraging a quantum computer, but it can be costly and complicated to implement.

Separate from QKD, PQC offers algorithms that are believed to be cryptographically strong, even with quantum computing. A range of approved PQC algorithms have been defined, and most regulatory bodies continue to support research to determine additional algorithms. Algorithms like ML-KEM are designed to withstand attacks from classical and quantum computers. These algorithmic changes can often be retrofitted into existing equipment via updated software.

Empowering Quantum Resilience with the Fortinet Security Fabric

One of the first steps in putting together a PQC migration plan is understanding your cryptography estate to identify where quantum-vulnerable cyphers are in use. Cryptography used in common systems might already be known (such as VPN connections), but there are places in enterprise networks where encryption is in use that may not be top of mind. Fortinet FortiManager and FortiNDR can help enterprises gain visibility and build a cryptographic checklist for data in motion across their networks. Once a solid understanding of where encryption that is not quantum-ready is in use, a plan for migration to PQC can be built that prioritizes systems with access to sensitive information first.

The FortiOS operating system provides the foundation for Fortinet FortiGate Next-Generation Firewalls and FortiSASE, allowing for quantum capabilities across both solutions. It supports PQC and QKD, including IPsec VPN tunnels and SSL deep inspection. Crypto-agility is provided via the ability to stack cryptography, combining existing PQC and QKD to ensure quantum-safe and operational resiliency.

Some malicious organizations have embarked on a strategy of "harvest now, decrypt later," intending to store sensitive data for five years or more, until the evolution of quantum empowers them to break the encryption.[2]

Along with your infrastructure, your endpoints will need to be capable of PQC. FortiEndpoint offers PQC, ensuring that FortiEndpoint-enabled devices can connect securely and pass data that is quantum safe.

Operational technology (OT) networks may not have the possibility to add PQC to their devices, exposing the data to HNDL attacks. The insertion of FortiGate in key points and segments in these networks ensures quantum-safe communications within and from the OT network.

FortiWeb web application and API protection and FortiADC application delivery controller support PQC for quantum-resilient key exchange and signature mechanisms in TLS 1.3.

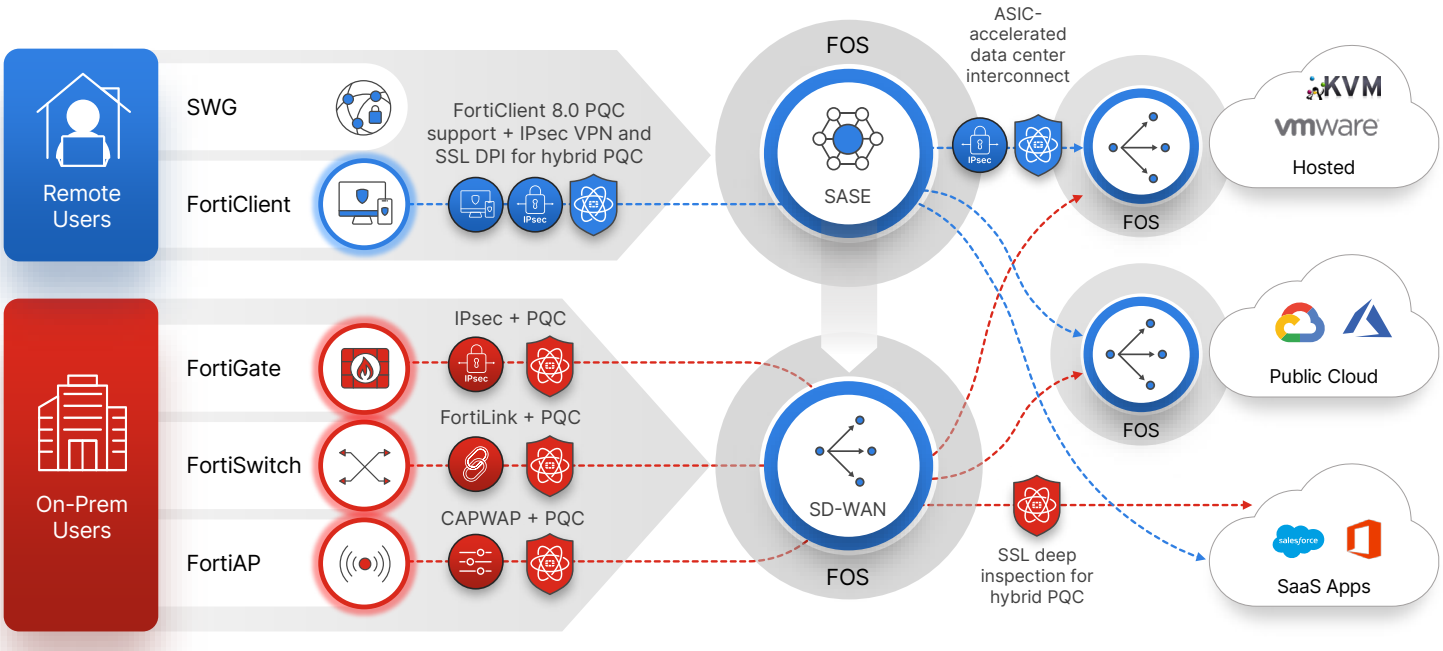

Figure 1: Enabling quantum-safe operations with FortiOS

The Fortinet Security Fabric can help organizations transition to quantum-safe cryptography while strengthening visibility and control to reduce risk exposure across networks and data. Capabilities such as endpoint protection, identity and access management, zero-trust network access, and data loss prevention all play a role in mitigating risk to data in motion and in use. The Fortinet Security Fabric empowers organizations to consolidate these controls into a unified, quantum-safe, AI-driven security platform.

Start Your Quantum-Safe Journey Today

As Q-Day approaches, you'll need to view and understand your cryptographic footprint so you can take action before it's too late. It's crucial to begin planning and adopting quantum-safe measures today.

The Fortinet Security Fabric offers integrated quantum-safe capabilities across the platform, allowing for robust security throughout your environment. Leveraging quantum-safe communication capabilities from Fortinet enables you to secure data and maintain regulatory compliance now and in the future.

[1] Brian Hopkins, David Mooter, Martha Bennett, Charlie Dai, Sandy Carielli, et al, The State Of Quantum Computing, 2026: Quantum Computers Are At An Inflection Point, Forrester, February 24, 2026. https://www.forrester.com/report/the-state-of-quantum-computing-2026/RES192193

[2] Gabe Dunn, Velu Sinha, Laurent-Pierre Baculard, Syed Ali, and Willy Chang, Quantum Computing Moves from Theoretical to Inevitable, Bain & Company, September 23, 2025. https://www.bain.com/insights/quantum-computing-moves-from-theoretical-to-inevitable-technology-report-2025/

Copyright © 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's SVP Legal and above, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

July 21, 2026 9:58 AM / MKTG-3810-0-0-EN