Post-quantum cryptography readiness

F5® Application Delivery and Security Platform enables a seamless transition to post-quantum cryptography across hybrid, multicloud, and legacy environments.

Key benefits

Streamline post-quantum cryptography readiness
Remove barriers to PQC preparation across diverse infrastructures while enabling app protection, API security, and operational efficiency wherever workloads reside.

Ensure crypto agility
Adopt standardized PQC ciphers as they evolve to avoid architectural overhauls while maintaining robust, proactive PQC readiness.

Defend against "harvest now, decrypt later" attacks
Protect your organization against future quantum threats with advanced encryption technologies.

Future-proof your security
Safeguard sensitive data with support for NIST-standardized PQC, enabling proactive threat mitigation while ensuring privacy, compliance, and data resilience.

Simplify end-to-end encryption
Minimize complexity and enable scalable, high-availability, PQC-ready encryption for apps and APIs across any environment to ensure a smooth transition without business interruptions.

The backbone of today's internet security that many of us rely on daily for online banking, secure messaging, and data protection will be severely compromised by quantum computing.

Quantum computing is a powerful opportunity and a looming threat

Quantum computing is one of today's most exciting technological advancements, poised to transform industries with its unparalleled processing power. Unlike classical computers, which encode data using binary bits (zeroes and ones), quantum computers leverage quantum bits, or qubits. Qubits can exist in a superposition of zero and one, meaning they can be a zero, a one, or a combination of both at the same time. This capability enables quantum computers to solve certain types of problems exponentially faster than today's classical computers.

While quantum computing won't necessarily benefit everyday tasks like web surfing, its true strength lies in addressing complex, data-intensive challenges, such as accelerating medical and pharmaceutical research, optimizing AI algorithms, improving network designs, and advancing cryptography.

The dark side of quantum computing

As promising as quantum computing is, its rapid advancements carry enormous risks—particularly for cryptography. Theoretically, quantum computing could break even the strongest encryption methods in use today, including Transport Layer Security (TLS) and Digital Signature Algorithm (DSA).

According to U.S. National Institute of Standards and Technology (NIST) and other leading researchers, quantum supremacy—the point when quantum computers surpass today's most advanced classical systems—could arrive by 2030. This breakthrough may render the cryptographic algorithms we rely on to protect personal data and secure communications completely obsolete.

To address this looming threat, NIST has been leading efforts to develop post-quantum cryptography (PQC) standards that can withstand the power of quantum computing. These evolving standards will play a critical role in protecting sensitive information as we transition to a quantum-ready future.

If current cryptographic methods are broken, the backbone of today's internet security—relied upon daily for online banking, secure messaging, and data protection—will be severely compromised. Sensitive information, such as personally identifiable information (PII), personal health information (PHI), government IDs, and other critical data could be exposed and exploited.

Key features

NIST-standardized algorithm support
Support critical NIST-standardized post-quantum cryptographic algorithms, both client-side and server-side.

Post-quantum readiness for all environments
Take advantage of security offerings optimized for enterprise PQC and ensure post-quantum cipher support across distributed environments for advanced application and API protection.

Hybrid cipher support
Leverage hybrid ciphers to ensure security flexibility and compatibility, with ciphers supported by both clients and servers.

Trustworthy, reliable availability
Address quantum computing challenges while ensuring long-term, dependable, resilient availability for critical data and applications.

Protection of post-quantum gaps
Use F5 ADSP as an intermediary to provide quantum-resistant handshakes even when client or server systems lag in PQC adoption.

The “harvest now, decrypt later” danger

The cryptographic risks of quantum computing aren’t confined to the future. Cybercriminals are already preparing for Q-Day—the moment quantum computers can break today’s encryption. Bad actors have adopted a “harvest now, decrypt later” strategy, stealing encrypted sensitive data today in anticipation of decrypting it in the quantum future.

Stolen information, ranging from government secrets to personal records, may retain its value for years or even decades, creating a persistent and escalating risk. Cybercriminals don’t need quantum computers yet—they're simply waiting for the technology to catch up.

The urgency is undeniable, and this danger isn’t hypothetical or far off. It’s unfolding right now.

Broader risks to infrastructure and security

The implications don’t stop at encrypted data. Quantum computing could disrupt critical infrastructure, including power grids and water systems, while leaving financial networks vulnerable to significant losses. Even sensitive government systems, especially defense and intelligence networks, could be at risk.

The stakes are amplified by a global race to dominate quantum computing. Nations, megacorporations, and even cybercriminal organizations are vying to develop quantum computing. The first to succeed will wield immense power and influence, but in the wrong hands, quantum capabilities could disrupt global security and economic stability.

Challenges to implementing quantum-resistant cryptography

Organizations face numerous roadblocks as they seek to transition to quantum resistant cryptography (QRC), including:

- **High costs and complexity:** Transitioning from existing cryptography to PQC is incredibly complex and can be costly and resource intensive.
- **Compatibility and interoperability issues:** PQC algorithms often use larger key sizes, which demand increased bandwidth and can create incompatibilities with legacy security solutions.
- **Performance concerns:** QRC algorithms are more computationally intensive, potentially leading to increased latency or degraded performance. This is particularly true when hybrid cryptography—which combines classical and quantum-safe algorithms—is deployed in application delivery solutions.

- **Evolving standards.** PQC standards are still in development. NIST has published draft algorithms (under FIPS-203), but organizations will need to adapt to changes as standards evolve.

Another key technical challenge involves the TLS handshake process, where PQC's larger key sizes may cause fragmentation. Once a TLS handshake is fragmented, downstream inspection devices that don't support PQC ciphers and algorithms may break. To address this, organizations should ensure TLS 1.3 is deployed across their systems as a first step.

Organizations should also focus on protecting sensitive, long-lived data by prioritizing PQC readiness. Critical information with lasting value—such as PII, PHI, or government IDs—should be safeguarded using PQC as a first step. Meanwhile, less sensitive data can continue to rely on TLS 1.3 with RSA, ECC, and other strong ciphers that are currently available. Adopting a phased approach that strategically blends PQC with existing encryption methods can help mitigate challenges of transitioning to PQC to every client or server.

Preparing for the quantum era

Preparing for Q-Day is a global challenge that affects nearly every industry. The time to act is now. Starting your transition to PQC today ensures your most critical assets remain secure as the quantum era unfolds. Success will require balancing the protection of long-lived sensitive data with the need for high performance and seamless user experiences for both enterprises and their customers.

F5 solutions deliver ease of use for simplifying crypto-offloading, high performance for demanding workloads, and the scalability required to efficiently manage even the most complex deployments.

F5 Application Delivery and Security Platform: Enabling crypto agility for enterprises

For years, enterprises have relied on industry-leading F5 cryptographic solutions to protect their applications with the latest encryption algorithms. F5 solutions deliver ease of use for simplifying crypto-offloading, high performance for demanding workloads, and the scalability required to efficiently manage even the most complex deployments.

Built-in cryptography for maximum agility

Cryptography is embedded into the core of the F5® Application Delivery and Security Platform (ADSP) via the F5 BIG-IP® Traffic Management Microkernel (TMM), a foundational element of BIG-IP solutions. The BIG-IP TMM:

- Centralizes management of cryptographic handshakes and encryption processes
- Enables crypto agility for easier adaptation to emerging cryptographic standards and strategies

- Supports quantum-resistant ciphers for both clients and servers, providing hybrid key encapsulation for robust PQC protection

Because of its pivotal role in network and application architectures—managing traffic between clients and servers—F5 ADSP is strategically positioned to facilitate and ensure PQC readiness while adapting seamlessly as encryption standards evolve.

Hybrid cipher support for flexible compatibility

F5 ADSP simplifies the transition to PQC by supporting hybrid ciphers that blend classical cryptographic algorithms (e.g., RSA and ECC) with quantum-resistant algorithms (e.g., Kyber). As a full proxy solution, F5 ADSP enables:

- Flexibility between privacy, security, and crypto compatibility based on the ciphers supported by clients and servers
- Seamless hybrid cipher support, ensuring secure communication across the network
- Quantum-resistant handshakes, enabling strong encryption—even when other devices in your stack haven't adopted PQC standards yet

By acting as an intermediary, F5 ADSP ensures enhanced protection across your network regardless of where clients or servers are in their PQC journey.

Performance optimization for PQC

PQC algorithms often use longer encryption keys and introduce greater computational complexity, which may increase latency. F5 ADSP addresses these challenges through:

- F5 appliance acceleration features that offset possible performance impacts caused by PQC
- An upgradable framework for cryptographic transformations, enabling seamless adoption of emerging PQC ciphers as they evolve
- The capability for organizations to retain direct control over their cryptographic resources and potentially expend less compute power addressing PQC compared to cloud-based providers

Comprehensive security across environments

In addition, F5 ADSP supports PQC ciphers when an OpenSSL engine with liboqs support is being used. It negotiates quantum-safe keys and uses quantum-safe authentication in TLS 1.3.

Plus, as a full proxy solution, F5 ADSP supports post-quantum ready ciphers, hybrid ciphers, and TLS 1.3 across your environments. By acting as an intermediary, F5 ADSP ensures an appropriate level of security for all your information, enabling resiliency of existing deployed cryptography with the ability to adapt as needed.

Conclusion

F5 ADSP equips you to meet today's TLS encryption needs with a flexible, efficient, and scalable solution that evolves as quickly as the cryptography it supports. With its comprehensive security and crypto agility, F5 ADSP helps you protect critical data, PII, PHI, IP, and more in the most secure and effective manner possible.

To learn more about how F5 is addressing PQC, read our blog series on the topic. You can also contact F5 to find out how you can start deploying PQC with F5 ADSP today.