Future-Ready Security: Preparing for the Quantum Era Today

Presenter Name (pronouns)
Title
Date

Modern Cryptography

“The path to a million-qubit processor is now within reach – bringing us closer to solving problems beyond the capabilities of classical computing.” – Microsoft CEO Satya Nadella Feb 2025

A geopolitical surprise could make this a fire drill we’ve seen coming for > 15 years.

Quantum computing will revolutionize technology and industries

Speed up drug discovery for cancer

Optimize energy grids and networks

Improve space exploration flight paths

QUANTUM COMPUTING

is an advanced type of computing

Classical computers

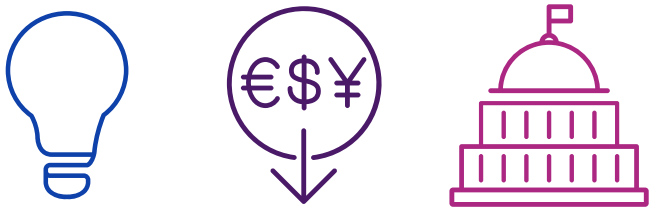
use 0's & 1's to encode data, while quantum computers use quantum bits, or qubits

Qubits

can be in a superposition* (they can be 0 or 1 or a combo of both at the same time)—this enables problems to be solved much faster

*Quantum mechanics principle describing a system able to exist in multiple states at the same time

The same power that brings opportunity also introduces enormous risk to cybersecurity



Quantum computing could threaten critical infrastructure (power grids, financial networks, government systems, etc.) if quantum-resistant security measures aren't taken

Nations and organizations in a race to develop quantum computing will wield immense power if they capture exclusive access to quantum capabilities

“ ”

To resist attacks from both classical and quantum computers, organizations must transition to post-quantum cryptography (PQC). But that’s hardly a simple switch. It will require more work than preparing for Y2K, and failure could have dangerous consequences.

GARTNER

  Source: Gartner, Begin Transitioning to Post-Quantum Cryptography Now, Sept. 30, 2024

Q-Day is Coming, Customer Data is Already at Risk

Classical encryption protects customer data today

Bad actors are running “harvest now, decrypt later” attacks

On “Q-day,” classical encryption won’t be enough to protect data

Your Opportunity:

Moving to Post-Quantum Cryptography Readiness *now* **can help customers get ahead of their competition** & regulatory standards

As a leader in cryptography innovation and app security, the F5 ADSP simplifies your path to PQC readiness.

DISCOVER

Evaluate your quantum risk

Inventory crypto-sensitive assets

Focus on high-risk assets to mitigate exposure while avoiding unnecessary performance overhead

Use the Application Study Tool to understand your fleetwide cipher use

TEST

Pilot quantum-resistant algorithms without disrupting apps

DEPLOY

Adopt TLS 1.3—have the framework for when it's time to fully adopt PQC

Seamlessly transition your encryption infrastructure—your high-risk, critical systems first—with hybrid cryptography

EVOLVE

Adapt to emerging PQC standards—quantum-safe cryptography is still evolving

Start with TLS 1.3 to enable a smooth, incremental shift to full PQC adoption

1

Adopt TLS 1.3 for immediate and downstream benefits

Implement TLS 1.3 for stronger security—TLS 1.3 doesn't just prepare you for quantum-safe encryption, it improves your encryption performance today.

2

Transition to PQC for critical inventory

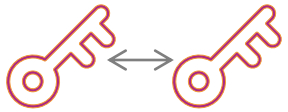
Start by securing what's most critical to reduce exposure without overwhelming resources or compromising performance across your organization.

3

Expand PQC as needed—but before "Q-day"!

Expand PQC incrementally to stay ahead of quantum threats and avoid rushed, resource-intensive migrations when Q-day gets even closer.

Post-quantum cryptography (PQC)



Includes a set of algorithms for handshakes, key exchanges, and signatures considered “quantum resistant”

Algorithms are designed to remain secure even with increased computing power of quantum computers – minimizing risk of cryptographic key compromise

BIG-IP

Starting in BIG-IP version 17.5.1, BIG-IP supports client-side **and** server-side, hybrid key encapsulation for post-quantum cryptography protection

NGINX Plus R33 supports PQC ciphersets today using the Open Quantum Safe provider library for 3.x

https://github.com/open-quantum-safe/oqs-provider

Post-Quantum Cryptography

Post-Quantum NIST Finalists

CRYSTALS

- **ML-KEM** ("Kyber" for general-purpose key encapsulation – TLS handshake)
  - X25519+Kyber768Draft000 (pre-FIPS Hybrid KEM)
  - X25519MLKEM768 (official #1 Hybrid KEM – FIPS 203)
  - SecP256r1MLKEM768 (official #2 Hybrid KEM – FIPS 203)
- **ML-DSA** ("Dilithium" for general-purpose digital signatures – FIPS 204)
- **SLH-DSA** ("SPHINCS+" for digital signatures – FIPS 205)
- **Falcon** (for digital signatures - DRAFT)

Post-Quantum Cryptography (PQC) Readiness

Problem:

Quantum computers will be able to break traditional encryption methods like RSA and ECC, exposing sensitive data.

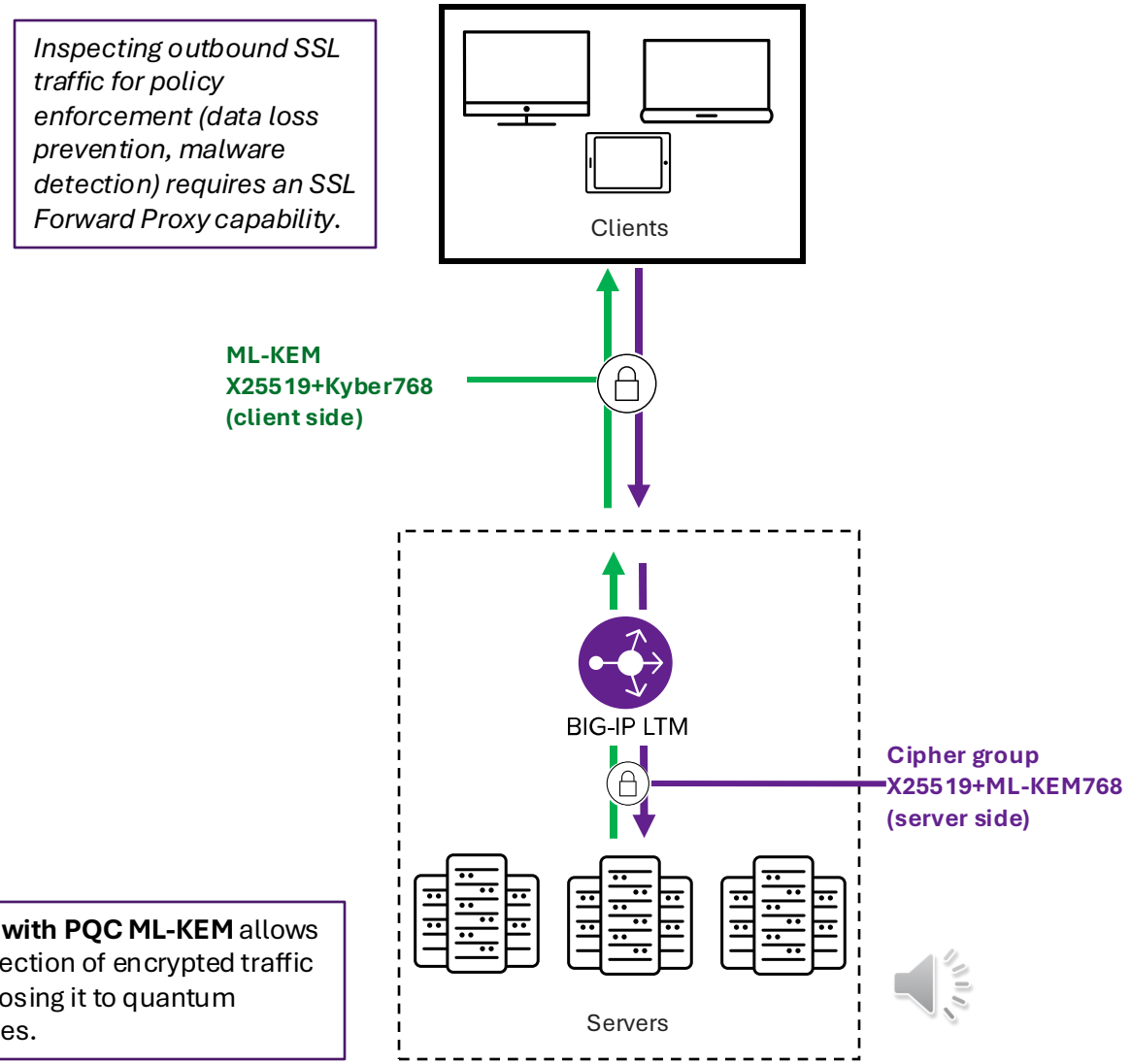
PQC uses algorithms that are expected to be secure even against quantum attacks (e.g., Kyber, Dilithium, BIKE, etc.)

Solution:

BIG-IP LTM supports **client and server-side post-quantum algorithms** for encryption of sensitive data

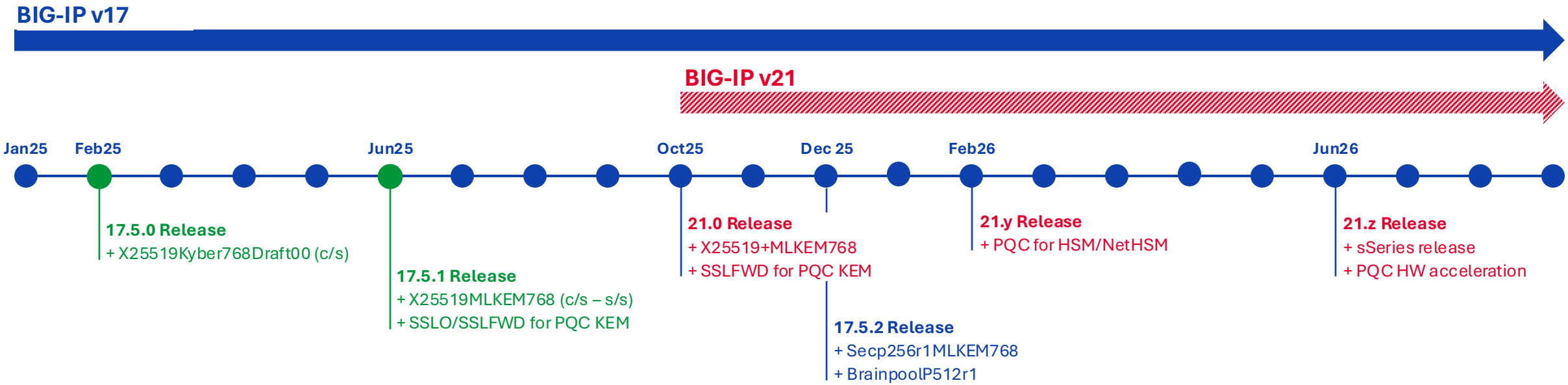
This means that data is encrypted using PQC-ready algorithms **from client to server to protect user data**

Even if clients or servers don't support PQC natively, **BIG-IP LTM can act as a PQC mediary** for both client and server.



Post-Quantum Cryptography

Roadmap Timelines (tentative)



TLS

#	Title	Use-Case	Business Impact
1	Client-side (decrypt) & server-side (re-encrypt) X25519+MLKEM768 algorithm support (FIPS203)	TLS 17.5.1	• Industries are aggressively moving towards quantum-resistant cryptography in preparation for Quantum Computing powerful enough to break classical algorithms. Conservative estimates put this event within the next 5 years, prompting high-stakes competition among technology vendors. • X25519+MLKEM768 represents the first "official" post-quantum cryptography (PQC) TLS handshake algorithm, standardized by NIST's FIPS203. • This also includes SSL Forward Proxy PQC handshake support.
2	Client-side (decrypt) & server-side (re-encrypt) SecP256r1MLKEM768 and SecP384r1MLKEM1024 algorithm support (FIPS203)	TLS 17.5.2	• PQC MLKEM handshakes with SecP represent a second set of NIST-specific hybrid MLKEM algorithms, in accordance with FIPS 203.
3	BrainpoolP512r1 and server-side SM2/SM3/SM4	TLS 17.5.1 (or 2)	• Brainpool is already supported on TMOS. This simply adds (requested) support for the larger version. • SM2/SM3/SM4 is already supported on TMOS for client-side. This simply adds (requested) server-side support.

4	OpenSSL upgrade	TLS	• OpenSSL on TMOS currently sits at 1.0.2, a very old and deprecated version. The implications of updating (or not updating) are as follows:
			  • Don't: Support for this old version costs F5 $50K/year.
			  • Don't: There is no guarantee that the OpenSSL org will be able to handle a next major vulnerability in the old versions of the libraries. It is a catastrophe waiting to happen.
			  • Do: Moving to the latest supported libraries will allow for rapid innovation of the newest cryptography, including PQC ML-DSA.
			  • Do: OpenSSL 3.0.x comes with FIPS certification baked in.

5	PQC ML-DSA support	TLS	• ML-DSA is the set of NIST-approved algorithms, provided in FIPS204, for TLS signature algorithms and authentication. As part of the aggressive move towards PQC, customers are continually asking for this on F5's roadmap. • ML-DSA will require the OpenSSL version update (see #4).
6	PQC support on BIG-IP management	TLS	• Customers are also asking for general (MLKEM and ML-DSA) support on the BIG-IP UI (and API).
7	Support for new/advanced algorithms	TLS	• Support for PQC HQC, SHA-3, Ed25519, and AEGIS (replaces AES).

More Resources

Reading

1. F5 Blog: Weighing in on the Post-Quantum Cryptography Hype
2. PQC “About” Page - NIST
3. PQC Standards Page - NIST
4. PQC Wikipedia Page
5. CISA PQC Initiative Page
6. 300-Level Product Page (PQC on LTM)
7. 200-Level Solution Page (PQC Readiness)
8. F5 DevCentral Article: PQC: Building Resilience Against Tomorrow’s Threats