White Paper

VIAVI Solutions

Preparing Security Infrastructures for Quantum-Safe Encryption

Preparing Security Infrastructures for Quantum-Safe Encryption

With the evolution of quantum computing occurring organizations across industries, from financial services and healthcare to government/defense and telecommunications, are evaluating Post-Quantum Cryptography (PQC) technologies to safeguard sensitive data. These sectors rely heavily on encryption to protect long-lived data and mission-critical transactions, making them early adopters of quantum-safe solutions. The urgency to future-proofing security infrastructures against quantum threats has become a top priority for CISOs, network security architects, and IT leaders worldwide.

Quantum computing advancements pose a significant risk to today's cryptographic methods, potentially rendering current encryption algorithms obsolete. Cyber adversaries are already employing "harvest now, decrypt later" techniques, collecting encrypted data today with the intent to decrypt it in the future using quantum capabilities.

Without proactive measures, sensitive data faces unprecedented vulnerabilities. Therefore, security teams adopting PQC must validate quantum-safe encryption algorithms to ensure infrastructure resilience, performance, and future-proof data protection.

Key Challenges

Quantum Readiness: Organizations must validate quantum-safe cryptographic methods to ensure seamless and effective implementation within their existing security infrastructures while maintaining optimal network performance.

Upgrade Planning: Businesses need to strategically identify and execute infrastructure upgrades to mitigate performance degradation and minimize any negative impacts on the Quality of Experience (QoE) for end-users.

Inspection Burden on Firewalls: Many enterprise-grade firewalls and security gateways rely on man-in-the-middle (MITM) inspection to decrypt and analyze encrypted traffic for malicious content. The introduction of quantum-safe encryption, which typically involves more computationally intensive algorithms and larger key sizes, significantly increases the processing load on these inspection systems. This can lead to latency, degraded throughput, or the need for costly hardware upgrades.

Interoperability: Not all services and servers will be able to support handshakes with other PQC enabled hosts, it's imperative that secure connection will fall back to a suitable cipher set automatically to maintain secure communication quickly and effectively with little impact to overall performance.

VIAVI CyberFlood – Leading the Way in PQC Testing

VIAVI CyberFlood, complemented by Avalanche support, stands as the industry's pioneering solution for comprehensive PQC cipher suite for advanced connection and performance testing.

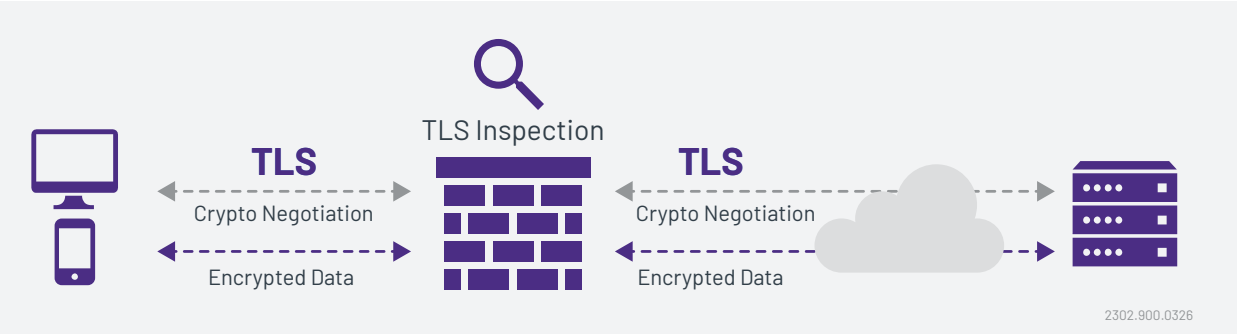
Industry Leadership: CyberFlood is the first-to-market solution offering complete support for PQC cipher suites compliant with the latest NIST FIPS 203, and FIPS 204standards.

Hybrid KEM Testing: The solution tests the **hybrid X25519MLKEM768** Key Encapsulation Mechanism (KEM), effectively validating robust fallback strategies, pinpointing interoperability challenges, and enabling smoother deployments.

HTTP Protocol Integration: PQC cipher suites are fully integrated into CyberFlood's extensive HTTP protocols, TestCloud Applications, ensuring validation under realistic, production-like traffic conditions.

PQC Cipher Coverage		
FIPS-203 Key Encryption Mechanisms (ML-KEM)	BIKEL1 BIKEL3 BIKEL5 FRODO1344AES FRODO1344SHAKE FRODO640AES FRODO640SHAKE FRODO976AES FRODO976SHAKE HQC128 HQC192 HQC256 KYBER1024 KYBER512 KYBER768 MLKEM1024 MLKEM512 MLKEM768 P256_BIKEL1 P256_FRODO640AES P256_FRODO640SHAKE P256_HQC128 P256_KYBER512 P256_KYBER768 P256_MLKEM512	P384_BIKEL3 P384_FRODO976AES P384_FRODO976SHAKE P384_HQC192 P384_KYBER768 P384_MLKEM1024 P384_MLKEM768 P521_BIKEL5 P521_FRODO1344AES P521_FRODO1344SHAKE P521_HQC256 P521_KYBER1024 P521_MLKEM1024 SECP256R1MLKEM768 X25519_BIKEL1 X25519_FRODO640AES X25519_FRODO640SHAKE X25519_HQC128 X25519_MLKEM512 X25519 MLKEM768 X448_BIKEL3 X448_FRODO976AES X448_FRODO976SHAKE X448_HQC192 X448_KYBER768 X448_MLKEM768

PQC Cipher Coverage		
FIPS-204 Digital Signatures (ML-DSA)	CROSSRSDP128BALANCED FALCONPADDED1024 FALCONPADDED512 MAYO1 MAYO2 MAYO3 MAYO5 MLDSA44 MLDSA44_BP256 MLDSA44_ED25519 MLDSA44_P256 MLDSA44_PSS2048 MLDSA44_RSA2048 MLDSA65 MLDSA65_BP256 MLDSA65_ED25519 MLDSA65_P256 MLDSA65_PSS3072 MLDSA65_RSA3072	MLDSA87 MLDSA87_BP384 MLDSA87_ED448 MLDSA87_P384 P256_FALCONPADDED512 P256_MAYO1 P256_MAYO2 P256_MLDSA44 P384_MAYO3 P384_MLDSA65 P521_FALCONPADDED1024 P521_MAYO5 P521_MLDSA87 RSA3072_FALCONPADDED512 RSA3072_MLDSA44 RSA3072_SPHINCSSHA2128FSIMPLE RSA3072_SPHINCSSHA2128SSIMPLE RSA3072_SPHINCSSHAKE128FSIMPLE



Validation of Man-in-the-Middle Inspection Capabilities

Benefits:

Validated Security Controls, Performance, and Interoperability: CyberFlood rigorously tests quantum-safe cipher implementation across encrypted traffic flows, firewall inspection scenarios, and hybrid KEM fallback mechanisms. This ensures that security policies remain effective, infrastructure components, including firewalls, proxies, and deep packet inspection engines, can operate under the added computational load of PQC, and that fallback interoperability with legacy systems is validated to ensure seamless transitions.

Future-proof Validation: The solution offers advanced, realistic testing methodologies designed to replicate genuine deployment environments, addressing all key challenges, from cryptographic readiness and compatibility issues to performance impacts on inspection-based security controls.

Strategic Confidence: The solution provides detailed insights and validation data that empower decision-makers, facilitating confident and informed planning for security infrastructure investments to combat future quantum computing threats.

Reduced Risk and Cost: By proactively identifying potential infrastructure gaps and performance issues ahead of widespread quantum computing adoption, organizations can significantly reduce security and compliance risk, minimize disruptions, make correct device deployment decisions, and control costs associated with future cryptographic transitions.

Organizations evaluating post-quantum cryptography (PQC) can use VIAVI CyberFlood to assess how quantum-safe encryption impacts network performance and security infrastructure. By supporting early implementations of NIST-compliant PQC standards and providing broad cipher suite coverage, CyberFlood enables teams to validate cryptographic readiness, identify potential interoperability issues, and gauge inspection performance under realistic conditions. As encryption protocols evolve, such testing helps inform upgrade strategies and supports long-term planning for secure and resilient operations.

For more information, please visit www.viavisolutions.com/en-us/products/cyberflood.

Contact Us: +1 844 GO VIAVI | (+1 844 468 4284). To reach the VIAVI office nearest you, visit viavisolutions.com/contact

sec-infrastructures-quantum-wp-hse-nse-ae
30195006 900 0326

viavisolutions.com