Quantum eMotion Expands Its Cybersecurity Portfolio with eShield-Q Gateway Capability, Targeting Today's AI-Driven Cyberattacks and Tomorrow's Quantum Threats

written by Raj Shah | November 10, 2026

Post-quantum VPN and firewall capability protects the keys inside the gateway itself, extending eShield-Q Hardened Container Images and the SecureKey Crypto Library into a platform built for the AI and quantum era

November 10, 2026 (Source) – Quantum eMotion Corp. (NYSE American: QNC) (TSXV: QNC) (FSE: 34Q0) ("QeM" or the "Company"), a provider of quantum-secure cybersecurity solutions, today introduced eShield-Q Gateway, a cloud-native post-quantum IPsec VPN and firewall capability within its eShield-Q platform.

eShield-Q Gateway is designed to connect cloud networks, business sites and remote users across AWS, Microsoft Azure and Google Cloud. In addition to protecting network traffic, eShield-Q Gateway is designed to protect cryptographic keys and operations within the gateway itself. Encryption keys stay software-encrypted in memory, key generation draws on true quantum entropy, and tunnels can add NIST-standardized post-quantum key exchange.

The Gateway capability extends the eShield-Q platform, which helps organizations address two converging threats: AI tools

that find and exploit vulnerabilities faster than teams can patch them, and quantum computers expected to break today's public-key encryption.

Why runtime protection and quantum readiness matter now

The largest cryptocurrency theft on record began with phishing but was carried out with AI tools (NYT, October 30, 2026). Industry leaders now warn that banks, wallet services and critical infrastructure should assume they are under attack (Yahoo Finance, November 7, 2026). The same report cites Bank of America research suggesting that "Q-Day," when quantum computers can break today's encryption, could arrive as early as 2030.

Government agencies are urging organizations to prepare now. On November 5, 2026, the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA) and the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) released joint guidance, *Post-Quantum Questions to Ask Your Vendors*. It helps security, procurement and vendor-management teams assess whether suppliers understand quantum risk, are transparent about their cryptographic implementations, and can support a timely transition to post-quantum cryptography. The agencies stress early vendor engagement, particularly before long-term contracts or cloud service agreements. eShield-Q is built to support those conversations. It uses NIST-standardized post-quantum algorithms, lets customers configure post-quantum protection connection by connection, and includes a cryptographic module now in FIPS 140-3 validation testing.

According to Google and Chromium security research, roughly 70% of serious software vulnerabilities stem from memory-safety flaws, and AI-driven tools are now finding new flaws even in heavily audited cryptographic software. Mandiant and Google

Threat Intelligence report sustained exploitation of VPNs, routers and other edge appliances, which often sit outside endpoint monitoring.

Attackers rarely need to break the encryption algorithm. Once they can read memory, they can take the keys. eShield-Q is built on an “assume compromise” model that protects keys while they are in use, so a breach does not automatically become a key theft.

eShield-Q Gateway: protecting the trust boundary

Gateways concentrate routing policy, authentication, certificates and live traffic keys in one place, which makes them prime targets. eShield-Q Gateway is designed as a deployable virtual appliance for site-to-site, remote-access, hybrid-cloud and multi-cloud connectivity. It combines four layers of protection:

- protection key material through SecureKey;
- hybrid post-quantum key establishment using ML-KEM;
- quantum-generated entropy through eFlux-Q;
- confidential-computing support on compatible cloud platforms.

SecureKey works across the whole gateway stack, so a memory-read flaw in one component does not automatically give an attacker the keys that protect the rest. It also stays active inside confidential-computing environments, guarding against threats that hardware isolation alone is not designed to stop.

Designed for cloud operations. Terraform modules support repeatable deployment to AWS, Azure and Google Cloud. Teams can manage the gateway through a web console, an OpenAPI-compatible REST API, a Python client or the command line. Day-to-day

security operations are supported by:

- separate management, WAN and LAN roles
- deny-by-default traffic policy
- role-based access with multi-factor authentication
- audit logging
- encrypted software updates

Target use cases include sovereign-cloud operators, defence and government networks, regulated industries, and AI infrastructure that links GPU clusters across hybrid environments.

A growing eShield-Q product line

The Gateway capability builds on two products that bring the same protections into applications and AI infrastructure.

eShield-Q Hardened Container Images are maintained application images with SecureKey runtime protection, quantum entropy integration and CVE hardening. They deploy through standard Docker and Kubernetes workflows. Images ship with a secure-by-default cryptographic policy, including hybrid post-quantum algorithms where supported, in FIPS-enabled and non-FIPS editions. The catalog includes NGINX, Apache HTTP Server, Envoy, HAProxy, Kong, PostgreSQL, MySQL, MongoDB, Valkey, Keycloak, Python, Node.js, Java and PHP, and continues to grow. For AI teams, these images protect inference gateways, training services and the data layers that hold feature stores and embeddings.

The SecureKey Crypto Library is the memory-secure engine behind the platform. It is available for commercial licensing to companies building security products and infrastructure. It plugs into existing applications as an OpenSSL 3 provider, often without code changes, and runs on x86-64 and ARMv8. SecureKey

has been integrated with NGINX, OpenSSH, strongSwan, PostgreSQL and Vector Packet Processing. It also protects RSA, elliptic-curve and post-quantum private keys, and adds self-tests, runtime code-integrity checks and fail-safe behaviour.

The SecureKey Cryptographic Module is currently listed by NIST as an Implementation Under Test as part of the FIPS 140-3 validation process since July 13, 2026.

Executive commentary

“AI has changed the economics of attack, and quantum computing will change the economics of encryption,” said Dr. Francis Bellido, Chief Executive Officer of Quantum eMotion. “With the eShield-Q Gateway capability, we are extending our protection of cryptography from the application and the chip to the network boundary. Our goal is to help customers defend against AI-driven intrusions today while building the quantum resilience they will need for Q-Day.”

“Most gateways encrypt the tunnel but leave the keys behind it exposed in memory,” said Wayne Teeple, Chief Technology Officer of Quantum eMotion. ” Protecting the encrypted tunnel is only part of the security challenge. Cryptographic keys themselves can become valuable targets if a gateway or application is compromised. eShield-Q Gateway is designed to protect key material while it is in use, combine hybrid post-quantum key establishment with quantum entropy, and operate within confidential-computing environments. The goal is to extend protection beyond the tunnel to the cryptographic operations that secure it.

Availability

QeM is currently engaging with prospective customers and partners regarding the eShield-Q Gateway capability ahead of

planned commercial availability.

We encourage organizations interested in the eShield-Q Gateway capability on AWS, Microsoft Azure or Google Cloud can contact us at info@quantumemotion.com.

eShield-Q Hardened Container Images will be available in FIPS-enabled and non-FIPS editions, and the SecureKey Crypto Library is available for commercial licensing.

Quantum eMotion will also present the eShield-Q portfolio at the World Quantum Cannes Festival on November 17-18, 2026.

About Quantum eMotion

Quantum eMotion Corp. is a quantum-secure cybersecurity company developing a comprehensive platform designed to protect data, communications and digital infrastructure against both current and emerging threats. The Company's technologies combine quantum-generated entropy, post-quantum cryptography, secure communications and advanced cryptographic key protection to support applications across cloud computing, artificial intelligence, financial services, healthcare, blockchain, government and critical infrastructure.

For further information, please visit our website at https://www.quantumemotion.com/
or contact us at: info@quantumemotion.com

Francis Bellido, Chief Executive Officer
514 956.2525

Cautionary Note regarding Forward-Looking Statements

This news release contains "forward-looking information" within the meaning of applicable securities laws. Forward-looking information is based on management's current expectations,

estimates, projections, assumptions, and beliefs as of the date of this release.

Words such as “anticipates,” “believes,” “expects,” “intends,” “plans,” “seeks,” “may,” “could,” “would,” “should,” “will,” “potential,” and similar expressions are intended to identify forward-looking information, although not all forward-looking information contains these identifying words.

Readers are cautioned not to place undue reliance on forward-looking information. Actual results and future events may differ materially from those anticipated. The Company undertakes no obligation to update or revise any forward-looking information, whether because of new information, future events, or otherwise, except as required by applicable securities laws.

Neither TSX Venture Exchange nor its Regulation Services Provider (as that term is defined in the policies of the TSX Venture Exchange) accepts responsibility for the adequacy or accuracy of this release.