Keeper Security Introduces Quantum-Resistant Encryption to Protect Against Future Quantum Threats

The leading enterprise security platform strengthens defences against today's cyber threats while preparing customers for the quantum computing era

LONDON, UNITED KINGDOM, February 25, 2026 /EINPresswire.com/ -- Keeper Security, the leading zero-trust and zero-knowledge Privileged Access Management (PAM) platform, today announces its solutions are now quantum-resistant. Keeper has integrated the Kyber key encapsulation mechanism across its platform, a quantum-resistant encryption algorithm approved by the U.S. National Institute of Standards and Technology (NIST).

Building on its long-standing reputation for using the industry's most trusted encryption standards, Keeper's integration of Kyber delivers dual protection – defending against cyber threats now, while preparing customers for the quantum computing future.

The Quantum Threat Is Real

Current encryption standards, such as RSA and Elliptic Curve Cryptography (ECC), remain strong against present-day adversaries, but they are not built to withstand the unique computational characteristics of quantum machines. Once operational at scale, quantum computers will be able to break these algorithms, rendering the public key cryptography that underpins current internet security obsolete.

The risk is already present through "harvest now, decrypt later" attacks in which cybercriminals capture and archive encrypted transmissions today with the intent to unlock them once quantum technology matures. That means sensitive information transmitted today, including financial records, health data and intellectual property, could be exposed years in the future.

Recognising this risk, NIST finalised Kyber in 2024 as one of the first post-quantum cryptography standards – urging organisations to begin adoption. In the UK, the National Cyber Security Centre has advised organisations to begin preparing for the transition to post-quantum cryptography, particularly where sensitive data must remain confidential for years to come. As the Department for Science, Innovation and Technology advances the UK's £2.5 billion National Quantum Strategy, quantum readiness is increasingly recognised as a board-level resilience priority.

Keeper's Proactive Defence

Keeper's implementation of quantum-resistant encryption in client-server communications reinforces its leadership in protecting privileged access, secrets, credentials and connections while aligning with the broader adoption of post-quantum standards by Apple iMessage, Signal, Google Chrome and Cloudflare, which began deploying similar protections in 2024.

"Public key cryptography, including RSA and ECC, still provides strong defence against modern threats, but quantum computing changes the rules," said Dr. Adam Everspaugh, Cryptography Advisor at Keeper Security. "Keeper's hybrid approach combines battle-hardened, elliptic curve primitives with Kyber's lattice-based cryptography. This layered defence ensures customers remain protected against today's attackers while also guarding their data from adversaries armed with quantum capabilities in the future."

Keeper's implementation of Kyber is crypto-agile, enabling rapid updates to cryptographic protocols while maintaining backward compatibility during software upgrades. By securing both the client-server authentication handshake and encrypted tunnels for data in transit, Keeper ensures its zero-trust, zero-knowledge architecture can evolve alongside emerging standards. Quantum-resistant cryptography is delivered automatically as customers upgrade to the latest release, requiring no configuration changes or user action to benefit from enhanced, future-ready protection.

"Cybersecurity cannot be reactive. Waiting for quantum computers to arrive before acting would leave organisations dangerously exposed," said Darren Guccione, CEO and Co-founder of Keeper Security. "Keeper's deployment of Kyber is about foresight – helping our customers build resilience that spans both the threats they face today and the seismic changes on the horizon. We are ensuring that sensitive systems, credentials and secrets remain secure for decades to come."

Keeper's adoption of Kyber reinforces its leadership in building secure, resilient infrastructure. This milestone adds to Keeper's long-standing track record of meeting the highest compliance standards, including SOC 2 Type II, ISO 27001, ISO 27017, ISO 27018, FedRAMP High Authorization, GovRAMP Authorization and FIPS 140-3 validation.

The deployment of Kyber-based quantum-resistant encryption is now live in Keeper's backend APIs and Keeper Commander, with mobile platforms coming soon and a phased expansion across the Keeper platform designed to ensure compatibility and performance at scale.

For more information about Keeper, visit http://www.keepersecurity.com/

###

About Keeper Security

Keeper Security is one of the fastest-growing cybersecurity software companies that protects thousands of organisations and millions of people in over 150 countries. Keeper is a pioneer of zero-knowledge and zero-trust security built for any IT environment. Its core offering, KeeperPAM®, is an AI-enabled, cloud-native platform that protects all users, devices and infrastructure from cyber attacks. Recognised for its innovation in the Gartner Magic Quadrant for Privileged Access Management (PAM), Keeper secures passwords and passkeys, infrastructure secrets, remote connections and endpoints with role-based enforcement policies, least privilege and just-in-time access. Learn why Keeper is trusted by leading organisations to defend against modern adversaries at KeeperSecurity.com (http://keepersecurity.com/).

Learn more: KeeperSecurity.com (http://keepersecurity.com/)

Charley Nash
Account Manager
charley@eskenzipr.com
Visit us on social media:
LinkedIn
Instagram
Facebook
YouTube
TikTok
X