

QWERX Announces General Commercial Availability of Enterprise Secure Perimeter Software

National Security-Grade Device Authentication Now Available to the Private Sector

MERRIFIELD, VA, UNITED STATES, June 26, 2026 /EINPresswire.com/ -- QWERX, Inc., a cybersecurity company that has patented technology to eliminate vulnerable static device credentials, announced the general commercial availability of QWERX Enterprise Secure Perimeter, its device authentication platform that replaces static credentials with dynamic ephemeral keys that rotate every few seconds and vanish after use. The announcement was made on [NYSE Live, broadcast from the New York Stock Exchange](#).



QWERX CEO Greg Cullison interviewed at NYSE Live on June 25, 2026

QWERX Enterprise Secure Perimeter is the first quantum-proof device authentication platform backed by R&D grants from Los Alamos National Laboratory to be offered for general commercial use. The technology, originally developed to meet the most demanding security requirements of U.S. national security environments, is now available to private sector enterprises managing networked devices with vulnerable static authentication credentials.

“

We were building better vaults for keys that should never exist. Today we bring national security-grade protection to every organization that needs it.”

Greg Cullison, CEO & Co-Founder, QWERX

Static device credentials — certificates, keys, and tokens that remain unchanged on enterprise networks for weeks or months — are the root cause of most network

breaches. Eighty percent of breaches involve credential theft or misuse, and the emerging threats of AI-powered attacks and quantum computing are accelerating the exploitation of static credentials at machine speed. QWERX Enterprise Secure Perimeter eliminates this attack surface

entirely by continuously rotating device authentication keys so there is nothing persistent for an attacker to steal, harvest, or replay.

“I was one of 22 million Americans whose most sensitive personal information was stolen in the Office of Personnel Management (OPM) breach, because an attacker captured a single static credential and used it to walk through the front door,” said Greg Cullison, CEO and Co-Founder of QWERX. “That experience made clear to me that the industry was solving the wrong problem. We were building better vaults for keys that should never exist in the first place. QWERX was founded to change that, and today’s announcement represents the moment we bring national security-grade protection to every organization that needs it. With quantum computing on the horizon and AI-powered attacks already operating at machine speed, the transition window for fixing device authentication is now, not after the next breach.”

The commercial release follows extensive validation in government and defense environments. QWERX received two sole-source contracts from Los Alamos National Laboratory — awards made without competitive bidding after the laboratory concluded QWERX was the only viable solution for its requirements. The technology was subjected to independent third-party penetration testing, which found no successful path of attack. In addition, QWERX has demonstrated live device authentication over the Starlink satellite network, with authentication keys rotating every three seconds from anywhere on Earth.

“Bringing QWERX Enterprise Secure Perimeter to general availability is the culmination of years of rigorous engineering, testing, and validation against the highest security standards in the world,” said Neil Cavezza, Chief Product Officer of QWERX. “This is not a prototype or a proof of concept. This is production-grade software that has been hardened through government lab validation, independent penetration testing, and real-world deployment. We have built a platform that protects IT, OT, and IoT environments simultaneously with a software-only deployment, which means organizations can begin securing their device authentication layer today without hardware changes or infrastructure overhauls. The product is ready. The threat is already here.”

The commercial availability announcement coincides with mounting regulatory urgency around quantum-resistant security architecture. The NSA’s CNSA 2.0 mandate requires all new National Security System acquisitions to support quantum-resistant cryptography by January 1, 2027, with compliance deadlines beginning as early as September 2026. Executive Order 14144, signed in January 2025, reinforced these timelines and codified the migration mandate in federal law. While CNSA 2.0 addresses the encryption layer, QWERX addresses the device authentication layer — a complementary requirement that most compliance frameworks do not yet mandate, but that faces the same quantum threat.

About QWERX

QWERX, Inc. is a Virginia-based cybersecurity company that has patented technology to eliminate vulnerable static device credentials with dynamic ephemeral keys that cannot be hacked. QWERX

Enterprise Secure Perimeter protects IT, OT, and IoT environments against AI-powered attacks and quantum threats alike with a software-only deployment. The technology was backed by R&D grants from Los Alamos National Laboratory. QWERX was a finalist at RSA Conference 2023 Launch Pad, is integrated with CrowdStrike, and has been recognized as a Northern Virginia Technology Council (NVTC) Tech100 honoree. [For more information, visit www.qwerx.co](http://www.qwerx.co).

Marketing

QWERX, Inc.

[email us here](#)

Visit us on social media:

[LinkedIn](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/922516817>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.