QWERX Enterprise Secure Perimeter

Continuous cryptographic defense for the autonomous-attack era.

Breaches now begin with credentials that never change. Static keys, long-lived certificates, and shared secrets are harvested from endpoints and replayed at machine speed, turning one captured secret into network-wide compromise in minutes. QESP eliminates the target: every device authenticates with an ephemeral, per-session identity that expires in seconds, so a stolen credential is worthless before it can be used.

What QESP Delivers

01 SECURE THE NETWORK

Cryptographically isolate every device with ephemeral, per-session identities.

- › Per-session ephemeral keys
- › Platform-native trust anchors
- › Cryptographic micro-segmentation
- › Halts lateral movement instantly

02 COLLECT INTELLIGENCE

Capture authenticated, device-level telemetry continuously for your SOC.

- › Tamper-evident telemetry
- › Real-time anomaly detection
- › Splunk / Sentinel / Chronicle
- › Ground-truth for ML defenses

03 SIMPLIFY IDENTITY

Replace brittle PKI, password rotations, and MFA fatigue with one identity fabric.

- › No passwords or shared secrets
- › Eliminate certificate sprawl
- › Reduce IAM operational burden
- › Quantum-resilient by design

How QESP Works

A continuous cryptographic handshake — every device, every session, every packet.

01 ENROLL

Platform-native identity ceremony. No passwords, no shared secrets.

02 DEPLOY QESP AGENT

Lightweight agent derives ephemeral keys continuously, per session.

03 AUTHENTICATE

Every connection cryptographically re-verified. No implicit trust.

04 OBSERVE

Authenticated telemetry streams to your SOC, exposing anomalies live.

Validated and Proven

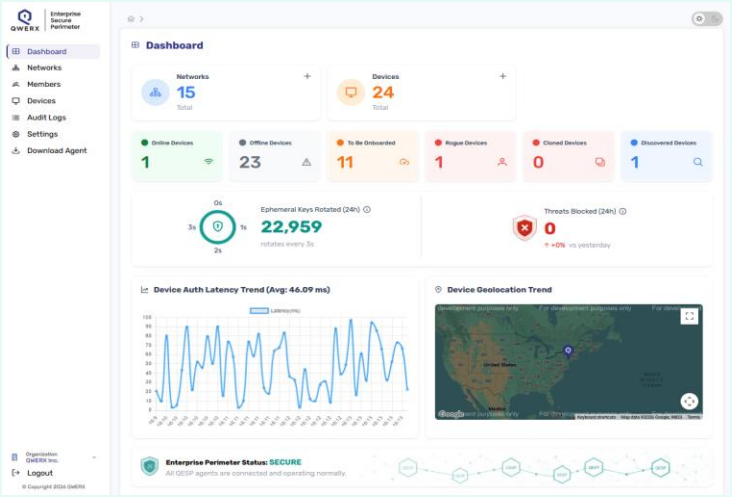
Government-validated. Independently tested. Patented quantum-proof protection.

- ✓ Los Alamos National Lab sole-source contracts
- ✓ 11 patents
- ✓ Assessed as quantum-proof by government research lab
- ✓ Independent PEN tests - no successful attack path
- ✓ Live demonstration over Starlink
- ✓ Listed on Tidal Cyber Vendor Registry (MITRE ATT&CK)
- ✓ Integrated with CrowdStrike Falcon Exposure Management
- ✓ RSA Conference 2023 Launchpad Finalist

LIVE OPERATOR CONSOLE

Real-time perimeter visibility. Every device, every key, every threat.

Ephemeral key rotation, blocked attacks, device health and geolocation streamed live to your SOC.



AI-Era Threats vs. QESP

How ephemeral cryptographic identity neutralizes the adversary's autonomous arsenal.

AI-ERA THREAT	WHY LEGACY DEFENSES FAIL	QESP RESPONSE
Deepfake & voice-cloned executive impersonation	Identity proofs assume a human is who they sound or look like.	Cryptographic device identity No human channel to spoof.
LLM-generated spear-phishing at scale	Users click. Credentials leak. AI weaponizes them in minutes.	No password to phish. Stolen tokens expire before use.
Autonomous lateral movement & ransomware	Flat trust zones let one foothold become full compromise.	Per-session keys isolate every device. No path to traverse.
Adversarial ML poisoning of detection models	Static signatures and behavior baselines drift and decay.	Authenticated telemetry provides tamper-evident ground truth.
Quantum-accelerated harvest-now-decrypt-later	Long-lived keys captured today are decrypted tomorrow.	Ephemeral keys are gone before quantum capability matures.
Stolen API tokens & service account abuse	Static bearer tokens grant durable, replayable access.	Cryptographic identity binds tokens to a live device session.
Supply-chain & insider compromise	Trusted insiders inherit broad, persistent privilege.	Per-session re-authentication revokes trust instantly.

Capabilities, Benefits & Specifications

Engineered for hostile environments.

CORE CAPABILITIES	CUSTOMER BENEFITS	TECHNICAL SPECS
Ephemeral key generation, per session	Eliminate credential breach vectors	Linux, Windows, macOS, embedded
Continuous device authentication	Halt lateral movement at first hop	x86_64, ARM64, edge & IoT
Cryptographic micro-segmentation	Reduce IAM and PKI burden	TLS 1.3, post-quantum hybrid
Authenticated telemetry pipeline	High-fidelity threat signal, live	Splunk, Sentinel, Chronicle
Hardware root-of-trust integration	Quantum-resilient by design	Hardware-rooted, tamper-evident
API-first SOC & SIEM integration	Faster Zero Trust compliance	REST + gRPC management APIs

Mission-Critical Industries

Deployed where compromise is not an option.

Defense & Federal Zero-trust enclaves, tactical edge	**Critical Infrastructure** Energy, water, pipelines, OT	**Financial Services** Stop credential theft & wire fraud
Healthcare Patient data, medical IoT	**Manufacturing & Supply** ICS/SCADA, robotics, suppliers	**Public Sector** Modernize without rip-and-replace

< 3s	0	100%	Minutes
KEY ROTATION INTERVAL	STANDING CREDENTIALS	AUTHENTICATED TELEMETRY	TO FIRST ENFORCEMENT

Engage QWERX

Deploy ephemeral identity across your enterprise.

Map QESP to your environment, threat model, and compliance objectives in under 30 minutes.
Contact Us: https://www.qwerx.co/contact