

Evolver SHIELD

Secure Hybrid Integrated Encryption & Lattice-ready Key Delivery

Enterprise-wide Quantum-safe protection without disruption.

Customer Challenge: Post-Quantum Cryptography Enterprise Security

U.S. Federal agencies and Fortune 500 enterprises must counter harvest-now, decrypt-later threats while modernizing cryptography—without disrupting networks, applications, or existing ATOs.

The practical requirement is a crypto-agile transition path that strengthens the network and application encryption, supports NIST PQC adoption as standards and vendor stacks mature, and requires no downtime, no packet rerouting, and minimal ATO churn.

Solution Overview

Evolver’s Secure Hybrid Integrated Encryption & Lattice-ready Key Delivery SHIELD is a post-quantum cryptography overlay that pairs Evolver’s cyber services with Quantum Xchange (QXC) Phio TX®. The platform is FIPS 140-3 and FIPS 203 (ML-KEM) validated for a practical, crypto-agile path adoption as technology stacks enable it.

Evolver Integrated Solution — Unique Features

Overlay, not forklift.

SHIELD strengthens existing data encryption by delivering out-of-band symmetric keys across copper/fiber/4-5G/satellite, preserving your network and app stack with no service interruption.

Crypto-agile by design:

policy enables algorithm agility and PQC insertion as vendor support lands—no architectural rework. Vendor-agnostic integration with multi-vendor networks and security products via standards-aligned interfaces and containerized deployment (including Cisco-native containers where supported).

Operational simplicity:

one pane manages key routing/mesh, continuous rotation, and multipath resilience; node licensing scales from enclave pilots to enterprise.

Assurance-first:

Evolver’s cyber RMF specialists produce boundary/CM/CP updates and delta-authorization packages to keep the overlay ATO-sustainable.

Evolver Provides

- Enterprise crypto inventory & discovery
- Pilot deployment
- Key-management modernization
- Crypto-agility policy, roadmap, and architecture
- ATO boundary updates, overlays, and continuous monitoring packages

Phio TX® provides Crypto Diversification™, including:

- Algorithm & software-stack redundancy
- Out-of-band symmetric key delivery
- Integration with existing VPN/SD-WAN and security stacks (no “bump-in-the-wire”)
- Key mixing and quantum entropy
- Support for encryption keys from any source: QKD, QRNG, PQC Deployment as software, container, or hardware (on-prem, AWS, Azure)

Expected Customer Benefits



Customers Gain:

- Immediate protection against quantum and classical cryptographic threats
- Extended life for existing VPN/SD-WAN and encryption investments
- A practical roadmap to enterprise-wide quantum readiness



SHIELD Provides:

- Package freshness
- Residual risk
- POA&M burn-down
- Enterprise coverage



Evolver’s Cyber GRC Experts Manage:

- Policy development
- Evidence generation
- ATO update cycles
- Continuous monitoring requirements



Programs Gain:

crypto-agility to adopt NIST PQC (e.g., ML-KEM-1024, HQC-128) as it becomes available in vendor stacks, with Evolver cyber governance, risk, and compliance professionals handling the policy, evidence, and ATO updates required for defensible authorization and continuous monitoring

How It Works

Crypto Discovery: Evolver starts with protocols, libraries, key lengths, endpoints and prioritizes high-value flows, and sets a crypto-agility policy (suites, rotation cadence, migration triggers).

Parallel Overlay Deployment: We deploy Phio TX® in parallel to existing tunnels/apps, creating an out-of-band key mesh over copper/fiber/satellite/4-5G—separate from the data plane—so routing is unchanged and no latency or packet loss is introduced.

SHIELD strengthens confidentiality by delivering a second symmetric key out-of-band and supports keys from QKD/QRNG/PQC sources, avoiding forklift changes to your VPN/SD-WAN/security stack.

Policy and Management: A GUI policy plane manages key routing, continuous rotation, and multipath; Phio TX® ships as software, container, or hardware for on-premises or cloud.

Upgrade and Alignment: Finally, Evolver updates ATO artifacts (overlays, key-management plans, rollback, POA&Ms), aligns continuous monitoring (telemetry, alarms, KPIs), proves performance in a pilot enclave, and scales in phases across enclaves and external connections.

Evolver Integrated Technology Solutions (EITS)

A portfolio of market-leading solutions for cybersecurity that accelerate federal missions delivered as modular capabilities that agencies can adopt quickly, integrate easily, and scale confidently. The EITS portfolio provides a cohesive suite of mission-ready technology accelerators designed to help federal programs improve speed, reduce operational burden, and increase measurable cybersecurity outcomes. Each solution can be deployed independently or combined to optimize customer operations.

SPECTRA SOC Support

An advanced AI-powered toolkit that enhances SOC results through high-fidelity detections, enriched telemetry, and governed automation to reduce analyst fatigue and operational cost

30-60 Day Pilot:

Bounded COI pilot with defined telemetry/parser tests, model governance, & SOAR runbooks; progress from advisory to enforced automation.

SHIELD Post-Quantum Cryptography

A transparent and portable solution for Post-Quantum Cryptography (PQC) enterprise network security, enabling agencies to safeguard critical tunnels with zero disruption and full auditability.

30-60 Day Pilot:

Pilot one or two critical tunnels; success = zero data-plane disruption, rotation SLOs met, policy/audit logs verified, and eMASS/CSAM artifacts updated; then phase rollout.

CLEAR Procurement

An expedited, non-intrusive, independent cybersecurity supply-chain risk assessment that accelerates vendor cyber risk assessments, improves visibility, and supports continuous risk monitoring at scale.

30-60 Day Pilot:

Pilot a supplier wave (25-50) to validate coverage, turnaround, closure KPIs; scale with continuous monitoring.

GUARDIAN Vulnerability Management

An integrated cyber risk-based vulnerability management solution tailored for U.S. Federal government programs to address fragmented and slow vulnerability management processes.

30-60 Day Pilot:

The pilot delivers a rapid, measurable advancement of an agency's vulnerability management maturity by unifying fragmented scanner outputs, normalizing exposure data, applying mission-aligned prioritization, and automating remediation workflows.

Procurement Options: *Existing Evolver GSA or agency services contracts *Public-sector channels/marketplaces (e.g., AWS Marketplace for CLEAR) *On-Prem/GovCloud deployment for SPECTRA/SHIELD per system boundary. 30-60-Day Pilots available.

Why Evolver

Who We Are

Our cyber teams work as partners focused on practical outcomes while leveraging AI and advanced data analytics tools to perform the work better, faster, and more cost-effectively, so authorization keeps pace with the speed of delivery.

Evolver delivers:

- End-to-end defensive cyber operations programs
- SOC operations
- Security engineering and architecture
- Cyber threat intelligence
- Penetration testing
- Cyber vulnerability scanning & analysis
- Cyber forensics analysis
- Cyber threat hunting
- AI/ML capabilities
- Full cyber governance, risk, & compliance (GRC) services
- Cyber-Supply Chain Risk Management (C-SCRM)



Gregory A. Garrett | Chief Operating Officer

Gregory.Garrett@cssoperations.com - 571.991.7768 - www.evolverinc.com