

# Evolver CLEAR

## Cyber Landscape Exposure & Assessment of Risk

*Independent, Accurate, & Timely Framework-Mapped Cyber-Supply Chain Risk Management (C-SCRM) Solution, with Clear Actionable Results.*

### Customer Cyber Challenge—Use Case

U.S. Government agencies and large commercial enterprises must rapidly assess and reduce third-party cyber risk, particularly across extended supply chains with numerous small and mid-sized suppliers. They must do this without:

- Relying on inaccurate supplier self-assessments
- Requiring intrusive cyber vulnerability scans
- Enduring long, manpower-heavy data review cycles

Business leaders need independent, accurate, timely, defensible, and framework-aligned assessments (NIST 800-171, ISO 27001, HIPAA/HITRUST, GDPR, SOC 2, PCI-DSS, CMMC) that can translate directly into procurement actions.

Traditional cyber risk self-assessment questionnaire-driven due diligence is slow, manpower intensive and inconsistent, while third-party assessments conducted on-site are time-consuming and too expensive. Neither are effective at driving continuous resilience in an AI-Attack environment.

### Solution Overview

Evolver Cyber Landscape Exposure & Assessment of Risk (CLEAR) pairs Evolver’s cybersecurity professional services with the WhiteHawk proven effective cyber risk-analytics platform, which delivers independent, fast, zero-intrusion supplier assessments, to multiple customer-selected cyber risk assessment frameworks at scale. The Evolver Cyber team and the Evolver Innovation Center have established a governed cyber supply chain risk management (C-SCRM) program leveraging the WhiteHawk cyber risk analytics platform.

- |  |   |
|--|---|
| Optional ingestion of supplier evidence                            | and dashboards  |
| Prioritized remediation playbooks                                  | Daily-updated framework-mapped scorecards                                 |
| Tiered requirements, supplier communications, acceptance criteria, | AI/ML-curated OSINT-driven cyber risk, compliance, and maturity analytics |

### Core Platform Capabilities and Process Flow

The platform produces framework-mapped scorecards and prioritized remediation playbooks updated daily while Evolver leads adjudication with suppliers, validates evidence, and tracks closure.

CLEAR supports both enterprise and SMB supplier ecosystems through flexible subscription models (including AWS Marketplace). It operates entirely off-premises and non-AI/ML-curated OSINT-driven cyber risk, compliance, and maturity analytics are typically delivered within 48 hours, depending on onboarding and volume. Output includes traceable findings, prioritized action plans, and executive summaries for acquisition and risk committees.

### Evolver Integrated Solution – Unique Features

#### Rapid, Non-Intrusive, Scalable Assessments

- No scans, no questionnaires, no supplier burden
- Scales to hundreds or thousands of suppliers
- Delivers consistent, defensible outputs

#### Framework-Aligned Content

- Configurable to agency baselines (NIST, ISO, CMMC pathways for SMBs)
- Supports continuous monitoring subscriptions—not one-time audits

#### Targeted SMB Enablement

- Virtual consults and automated assessments
- CMMC-mapped pathways
- Practical, budget-aware remediation roadmaps

#### Evidence-Lean for Suppliers, Evidence-Rich for Customers

- OSINT enriched by reputable next-generation data partners
- Clear, corroborated signals without intrusive data collection

### Expected Customer Benefits

#### Agencies & Enterprises Achieve:

- Faster onboarding and qualification of suppliers
- Stronger visibility into third-party cyber risk
- Improved framework alignment (NIST, CMMC, ISO)
- Prioritized, trackable remediation actions

#### Leadership Gains:

- Portfolio-level transparency
- Coverage by tier
- Remediation burn-down
- Residual risk trends
- Coverage by exceptions

#### CLEAR enables

independent, timely, and defensible acquisition and sustained third-party cyber risk management – better, **90% faster**, and **50% cheaper**.





## How It Works

- The Evolver cyber team establishes the governance model and tiered control expectations and onboards suppliers in waves.
- For each supplier, the platform runs OSINT-based analytics, maps exposures to applicable cyber risk frameworks, and issues a defensible scorecard with a ranked action plan.
- The Evolver cyber team leads adjudication to validate high-impact findings, align remediation, and set check-backs.
- All artifacts and metrics roll up to an executive dashboard tracking coverage, residual risk, remediation velocity, and cyber risk framework alignment, supporting reviews and acquisition gate decisions.

## 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.

### 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.

### CLEAR

#### Supply Chain

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.

### 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.

### 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.

### 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.

## 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

