Evolver Integrated Solution Paper (EISP)

Evolver GUARDIAN

An Integrated Enterprise Cyber Risk-Based Vulnerability Management Solution

Threat Prioritization and Compliance Management for Advanced Vulnerabilities

Customer Challenge: Cyber Risk Vulnerability Management

U.S. Federal government programs face increasing pressure to mature cyber risk vulnerability management. Today, most environments remain fragmented—multiple scanners, inconsistent severity ratings, unclear ownership, and slow remediation cycles. The result is missed patch windows, delayed vulnerability fixes, and lagging updates to security documentation.

Solution Overview

Evolver's GUARDIAN is a Cyber Risk-Based Vulnerability Management (RBVM) solution that combines Evolver's proven GRC and RMF services with Nucleus Security's FedRAMP Moderate Authorized Unified Vulnerability & Exposure Management platform. Together, they deliver a closed-loop RBVM capability that:

- Unifies cyber risk exposure data
- Prioritizes by cyber threat, asset criticality, and control impact
- Automates cyber risk tracking through remediation
- Exports evidence to RMF artifacts (eMASS, OSCAL, POA&M)

Nucleus ingests normalized, deduplicated data from more than 160 scanners and tools. Evolver overlays outcome-driven cyber services—RMF sustainment, POA&M management, and vulnerability governance—mapped to mission and enclave needs.

Evolver Integrated Solution – Unique Features

FedRAMP-Ready Platform + Expert GRC/RMF Services
- Government-authorized technology plus federal GRC/RMF operationalization

Tool-Agnostic, 160+ Native Connectors
- No scanner replacement required—rapid integration across environments

Mission-Tied, Threat-Fused Prioritization
- Combined exploitability, exposure, and RMF-informed impact scoring

POA&M & Compliance Management Automation
- Reduces manual effort and accelerates compliance evidence delivery

Institutionalized, Sustainable Program
- Embedded training ensures continuity, supporting workforce development mandates

Expected Customer Benefits

- Faster, measurable risk reductions, including up to 80 percent triage reduction and 50 percent fewer high-risk vulnerabilities within 90 days.
- Enterprise-wide visibility for ISSOs, CISOs, and mission owners.
- Lower Mean Time to Respond (MTTR) and Reduced Action Plan backlog via clear ownership and automation.
- Stronger ATO sustainment with aligned evidence and continuous-monitoring artifacts.

How It Works

Phase 1 – Baseline Onboarding (Days 0–30)

- Evolver conducts rapid VM/GRC intake across scanners, inventories, and enclave boundaries
- Nucleus software connectors ingest and normalize findings with no rip-and-replace
- Asset hierarchies and mission tags configured
- Initial dashboards and top-risk backlogs shared with ISSOs/CORs

Phase 2 – Prioritization & Automation (Days 30–90)

- Nucleus software fuses real-time threat intelligence
- Evolver implements RBVM governance: risk scoring, SLAs, exception workflows
- Automation configured for ticketing, ownership, POA&M rollups, and reporting
- Multi-tenancy support for enclaves or bureaus with risk-based oversight

Phase 3 – Scale & ATO Evidence (Days 90–180)

- Expanded to all approved enclaves and cloud/on-prem assets
- Nucleus software supports FedRAMP Software-as-a-Service (SaaS) and on-premises deployments
- POA&M and control alignment maintained in eMASS/OSCAL
- Scorecards and risk-acceptance reviews institutionalize governance

Phase 4 – Sustainment & Modernization (Ongoing)

- Evolver trains Government staff alongside execution
- Annual recalibration of models and tools ensures compliance with STIG CVM and ATO cycles

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.

ELEVATE

ATO Operations

Facilitates and expedites continuous ATO operations by unifying artifacts, automating evidence collection, and producing compliant outputs for agency systems of record.

30-60 Day Pilot:
Onboard read-only connectors, run a delta-authorization on a real change, validate OSCAL export, and AO feedback

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.

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.

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.

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