Evolver ANALYZE

Software Supply Chain Security & SBOM Assurance

Customer Software Security Challenge

Federal agencies still lack visibility into what is actually running on open-source software.

Existing tools fall short as Software Bill of Materials (SBOM) reflect declared manifests rather than compiled reality, scanners cannot reach firmware or embedded systems, and security tools stop at the container boundary. Recent supply chain compromises such as Trivy, LiteLLM, and Axios unfolded within days, impacting roughly 200 million weekly downloads and enabling large-scale data exfiltration. Under M-26-05, agencies must verify software integrity themselves rather than rely on vendor claims.

Solution Overview

Evolver ANALYZE combines Evolver's cybersecurity expertise with the NetRise platform, a CISA CDM APL-listed solution deployed across NNSA, CISA, and DHS. ANALYZE delivers deep visibility and continuous supply chain assurance across enterprise environments. The platform:

- Analyzes more than 200 artifact types including applications, containers, firmware, and devices with no source code, agents, or vendor support
- Generates SBOMs from compiled binaries that reflect runtime reality
- Maps full enterprise blast radius for emerging threats in minutes
- Detects vulnerable components rapidly, reducing exposure windows by months
- Identifies embedded credentials, weak cryptography, and AI components
- Exports evidence to RMF artifacts including eMASS, OSCAL, and POA&M and integrates with CDM pipelines
- Integrates with Evolver CLEAR for vendor risk and GUARDIAN for vulnerability management, creating a closed-loop lifecycle from procurement through sustainment

Evolver Integrated Solution — Unique Features

Federal-Authorized Platform and Mission Deployment
Binary analysis platform listed on the CISA CDM APL and deployed across NNSA, CISA, and DHS, combined with Evolver operational expertise

Binary-Level Visibility Across All Artifact Types
Analyzes compiled software, firmware, containers, and embedded systems including OT, ICS, PLCs, HMIs, and air-gapped environments

Full Blast Radius Mapping
Single-query impact analysis across containers, virtual machines, firmware, and physical devices

Pre-CVE Detection
Identifies vulnerabilities before public disclosure. Continuous monitoring detects risk as it enters the environment

Exploit-Aware Prioritization
Focuses remediation on reachable, auto-executing components. Reduces triage noise by up to 80% and accelerates mitigation

SBOM Validation and Provenance Intelligence
Validates vendor SBOMs. Maps dependencies across code, pipelines, and workflows

AI and Post-Quantum Cryptography Discovery
Identifies AI models, frameworks, and quantum-vulnerable cryptography across all artifacts. Supports NSM-10 and CNSA 2.0

Continuous Compliance and Evidence Automation
Automates RMF evidence generation and POA&M alignment

Operational Controls
NetRise operates as a SaaS or on-premises platform, with optional deployment in government-approved enclaves for classified or air-gapped environments

Expected Customer Benefits

Blast Radius in Minutes, Not Weeks
When a Log4j-class event lands, a single query returns every affected system.

Up to 80% Triage Reduction
Exploit-aware prioritization and reachability filtering eliminate noise so teams act on what is actually exposed.

Binary-Verified Inventory
Verified, ground-truth SBOMs across firmware, applications, containers, OT, and AI workloads, including HVAs and legacy platforms.

Accelerated Compliance
Automated evidence for EO 14028, OMB M-22-18, M-26-05, NIST RMF, NSM-10, CNSA 2.0, and CISA directives.

How It Works: Evolver deploys ANALYZE in a phased approach, integrating the NetRise Platform with Evolver's cybersecurity.

Phase 1: Days 0-30	Phase 2: Days 30-60	Phase 3: Days 60-120	Phase 4: Ongoing
Baseline Onboarding - Software asset intake across firmware, applications, containers, and device catalogs - NetRise ingests compiled binaries and generates binary-derived SBOMs - Initial vulnerability correlation, exploit-aware scoring, and HVA prioritization - Baseline blast-radius dashboards shared with ISSOs and CORs	**Validation & Prioritization** - SBOM validation against vendor-declared manifests and CDM data pipelines - Reachability and exploit-aware prioritization applied - C-SCRM governance: risk scoring, SLAs, and exception workflows - Provenance mapping of open-source components, GitHub Actions, and transitives	**Integration & Compliance** - Findings feed GUARDIAN for vulnerability management and CLEAR for procurement - POA&M and control alignment in eMASS/OSCAL with continuous evidence capture - Continuous monitoring for new deployments, firmware updates, and AI components - ATO evidence packages and PQC migration sequencing produced	- **Sustainment & Expansion** Government staff trained alongside execution - Continuous binary analysis of new releases and firmware - Real-time blast-radius response, emergency directives, and supplier designations - Annual recalibration of risk models, SBOM governance, and compliance posture

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

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.

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.

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.

ANALYZE
Software Supply Chain Security

An enterprise-wide solution for open-source software supply chain security, providing a detailed Software Bill of Materials (SBOM) visibility and continuous software supply chain assurance across enterprise environments.

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 Zero Trust 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)