NETRISE

Data Sheet

NetRise + EO 14306

Support EO 14306 objectives for secure software development, supply chain transparency, cryptographic visibility, and risk-prioritized updates with NetRise.

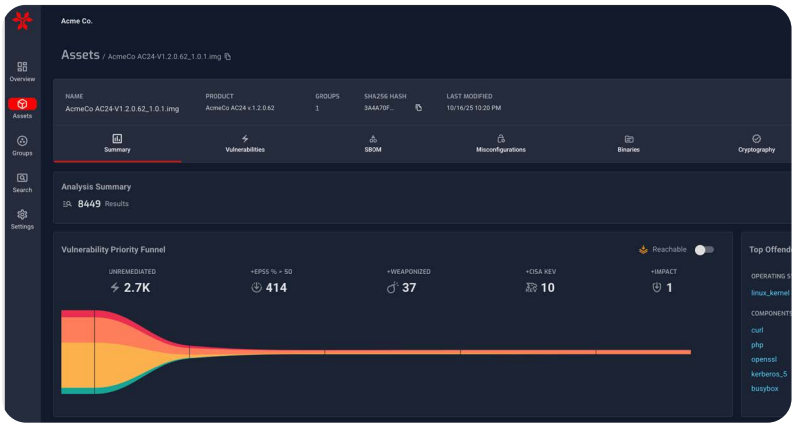
NetRise gives federal agencies and their vendors visibility into compiled software, supply chain provenance, and code vulnerabilities, helping agencies meet EO 14306 objectives for secure software delivery, patching, and risk-based prioritization of vulnerabilities.

EO 14306 strengthens requirements around secure software development, patch/update reliability, supply chain transparency, cryptographic visibility, and AI-related risk. NetRise helps agencies operationalize these objectives with binary-level evidence and behavioral analysis.

What the EO Demands. What NetRise Delivers.

Requirement Area	EO Context	What NetRise Provides
Secure software development evidence	Agencies must ensure secure development practices (e.g., SSDF-aligned guidance).	Binary-derived SBOMs; visibility into compiled code, configs, scripts; audit-ready reports.
Patch / update governance	Mandates emphasize secure, reliable updates and validation.	Scan and track patches and updates.; see how they change risk; prioritize by startup reachability.
Supply chain transparency (SBOM + provenance)	Greater transparency for third-party/OSS/embedded components.	Generate/enrich/validate SBOMs; lineage, licensing, provenance; verify vendor SBOMs.
Operational prioritization (what actually executes)	Move beyond checkbox compliance to operational risk reduction.	Startup/autorun reachability; exploit-aware vuln intel to focus on what's truly exposed.
Cryptography visibility	Agencies must plan crypto modernization.	Inventory and validate certs/keys/ crypto artifacts in binaries and packages.
Reporting & audits	Agencies need audit-ready evidence for oversight.	Compliance-readiness reports mapped to EO 14028, NIST CSF, EU CRA (and similar).

Operationalizing EO 14306 with NetRise



Beyond feature alignment, partnering with NetRise drives measurable outcomes that help federal agencies turn EO 14306 mandates into day-to-day practice.

Secure Development Evidence

Produce binary-derived SBOMs and audit-ready reports to demonstrate SSDF-aligned practices and satisfy agency oversight requirements.

Reliable Patch & Update Validation

Verify that updates remediate vulnerabilities, detect misconfigurations, and provide evidence for NIST SP 800-53 patching controls.

Supply Chain Transparency

Expose hidden third-party components, validate vendor SBOMs, and surface lineage data to strengthen acquisition reviews and supplier due diligence.

Operational Risk Prioritization

Identify which vulnerabilities are exploitable at startup or runtime, enabling risk-based decisions rather than checklist compliance.

Cryptography Insights

Inventory certificates, keys, and cryptographic libraries within software to support agencies' cryptographic modernization and EO 14306 compliance planning.

Audit-Ready Compliance Evidence

Generate structured reports aligned with EO 14028, EO 14306, NIST CSF, and the EU CRA to streamline audits and oversight reviews.

Features & Benefits

Binary Composition Analysis

Dissect compiled software to find hidden libraries, secrets, unsafe dependencies, without the need for source code.

Startup Risk Prioritization

Identify which vulnerable or risky components execute at boot/ startup, to prioritize patches.

Vendor & Component Provenance

Map third-party and embedded components, track where they came from and known vulnerabilities.

Patch Governance & Impact

See how patches and updates change risk and verify new versions don't re-introduce risk.

Execution-Aware Behavioral Analysis

Use intent-driven search and execution-aware reachability to uncover risky behavior and focus on what actually executes, supporting EO 14306 AI-related software risk objectives.

Cryptography Inventory

Identify and validate certificates, keys, and crypto libraries to inform modernization planning.

Tailored Solutions for Your Role

- **CISO / Chief Security Officer**
  Produce audit-ready evidence (binary-derived SBOMs, startup reachability, patch impact) to support EO 14306 objectives and oversight.
- **Software Development / OEMs**
  Integrate vulnerability scanning and binary analysis into CI/CD for "secure delivery of software."
- **Supply Chain / Vendor Risk Teams**
  Gain visibility into third-party component provenance and risk-tier categorization.
- **Risk / Audit Officers**
  Generate actionable evidence rather than attestations—binary-based verification helps audits under EO mandates.
- **Procurement Officers**
  Verify vendor claims, support supply chain transparency requirements.
- **Ops / DevSecOps Teams**
  Rapid detection of risky dependencies, tools, or malicious inserts in compiled code.

Deploy with Ease

Onboard Quickly

Start assessing your compiled software and binaries in hours.

Integrates with Existing Pipelines

Connect to CI/CD and build environments to generate SBOMs and surface risk automatically.

Continuous Monitoring & Reporting

Keep compliance status visible over time, not one-off snapshots.

Explore Platform Coverage

The NetRise Platform Coverage Sheet provides visibility into software, firmware, binaries, and embedded components—including cryptographic artifacts and AI-related software—helping agencies support EO 14306 objectives for secure software delivery and supply chain security.

Who Uses NetRise?

Government Agencies
Support EO 14306 objectives in acquisitions and contracts with binary-derived evidence.

DoD Software Teams
Align with patch/update requirements and secure startup integrity.

Contractor Vendors
Provide evidence of secure software development and supply chain transparency.

AI/ML Developers
Identify risky functionality in AI-related software artifacts and supporting code.

Cyber Threat / Incident Response Teams
Quickly discover indicators of compromise in binaries.

What's Inside *Your* Software? Let's Find Out

