SOLUTION BRIEF

REVERSINGLABS

Mission Assurance through Software Assurance

How Spectra Assure Operationalizes the Department of Defense Zero Trust Framework in the Software Supply Chain

Enabling DoD Zero Trust in the Software Supply Chain

As outlined in the Department of Defense (DoD) Zero Trust Strategy, no software application can be inherently trusted, and every component must be continuously inventoried, validated, and authorized.

Traditional methods, such as vendor questionnaires, penetration tests, or partial code scans cannot scale to meet this demand or produce the evidence required for Authorization to Operate (ATO).

ReversingLabs Spectra Assure® provides binary-level validation of software, generating SBOMs, verifying provenance, and assessing risk consumable by ATO and governance systems. This operationalizes Zero Trust principles for DoD acquisition and sustainment, ensuring mission software is safe to deploy and maintain.

Zero Trust Alignment: Applications and Workloads

APPLICATION INVENTORY

Requirement: DoD agencies must inventory and validate all third-party software to ensure visibility across mission systems.

Spectra Assure Capabilities:

- Generates complete SBOMs, including (AI, SaaS, and cryptographic components) directly from binaries—no source required
- Validates digital signatures and confirms provenance for each component
- Identifies embedded dependencies, cryptographic assets, and packaged libraries
- Produces machine-readable reports consumable by DoD asset systems

Mission Benefit: Trusted, complete inventories eliminate blind spots and enable rapid, evidence-based response when new vulnerabilities or threat intelligence affect deployed mission software.

SECURE SOFTWARE DEVELOPMENT AND INTEGRATION

Requirement: Buyers must verify that vendors follow secure SDLC and integration practices.

Spectra Assure Capabilities:

- Performs binary validation to detect tampering, injected malware, and exposure of secrets
- Performs behavior analysis to expose misuse of permissions and reveal embedded payloads
- Tracks provenance (supplier and authorship) for risk evaluation
- Generates reports providing objective, evidence-based assurance of vendor practices

Mission Benefit: Reduces the risk of adversary insertion into mission systems by ensuring software delivered to DoD programs has not been altered in the supply chain.

SOFTWARE RISK MANAGEMENT

Requirement: Programs must evaluate the risk posture of vendor applications before deployment and throughout their lifecycle.

Spectra Assure Capabilities:

- Provides automated binary risk scoring aligned to NIST SSDF, EO 14028, and DoD ZT standards
- Detects injected malware, embedded vulnerabilities, and misconfigurations
- Highlights novel risks introduced between software versions
- Supplies security levels and evidence-based scoring to support repeatable risk decisions

Mission Benefit: Enables faster, defensible risk determinations that accelerate secure acquisition without lowering assurance.

RESOURCE AUTHORIZATION AND INTEGRATION

Requirement: Vendor applications must be securely authorized and integrated with standard evidence for ATO and governance workflows.

Spectra Assure Capabilities:

- Supplies standardized SBOM outputs and attestations for ATO and integration systems
- Integrates with DevSecOps pipelines, SIEM/SOAR, and acquisition platforms
- Automates policy-driven gatekeeping (“deny by default”) to block unverified components
- Provides machine-readable compliance artifacts to accelerate authorization

Mission Benefit: Shortens ATO timelines and reduces rework, accelerating secure deployment of capabilities into operational environments.

CONTINUOUS MONITORING AND ONGOING AUTHORIZATIONS

Requirement: Assurance must be ongoing. Every update, patch, and release requires re-verification.

Spectra Assure Capabilities:

- Continuously analyzes new builds, patches, and updates for authenticity and integrity
- Verifies update provenance and confirms the authenticity of the software release
- Performs differential analysis to detect newly introduced risks
- Generates updated attestations to sustain ongoing authorizations

Mission Benefit: Preserves mission continuity by detecting risks as they emerge, enabling rapid mitigation without operational disruption.

Software Assurance Is Mission Assurance

Spectra Assure enables DoD agencies to apply Zero Trust principles directly to the software supply chain. By validating binaries, generating SBOM, confirming provenance, and enforcing continuous monitoring, DoD programs can securely acquire, authorize, and sustain mission software—ensuring resilience, readiness, and operational advantage.

Framework Quick Reference

Zero Trust Capability	DoD Requirement for Software Procurement	How RL Fulfills Requirement	Benefit to DoD Mission
Application Inventory	Agencies must inventory and continuously validate all third-party software.	Generates SBOMs and extended BOMs (including AI, SaaS, and Crypto components) from binaries; validates digital signatures and provenance.	Provides commanders and acquisition officers with a trusted inventory, reducing blind spots and enabling rapid response to vulnerabilities.
Secure Software Development & Integration	Buyers must verify that vendors follow secure SDLC and integration practices.	Confirms provenance, detects tampering or injected malware, validates reproducible builds, and produces SAFE reports.	Strengthens trust in vendor solutions by ensuring the software has not been altered—reducing the risk of adversary insertion.
Software Risk Management	Agencies must evaluate the risk posture of vendor applications.	Analyzes binaries for malware, vulnerabilities, and exposure of secrets; delivers repeatable software risk scores aligned with NIST and DoD ZT policies.	Enables mission owners to quickly assess relative software risk and prioritize approvals, thereby accelerating secure acquisition.
Resource Authorization & Integration	Buyers must ensure vendor applications can be authorized and integrated securely.	Supplies standardized SBOM outputs and attestations; integrates with DevSecOps, SIEM/SOAR, and acquisition platforms.	Accelerates ATO timelines with trusted artifacts, reducing deployment delays of secure capabilities.
Continuous Monitoring & Ongoing Authorizations	Agencies must maintain assurance with ongoing risk checks and re-authorizations.	Continuously re-validates patches and updates, detects new risks via differential analysis, and generates attestations for compliance.	Preserves mission continuity by ensuring software remains safe throughout its lifecycle, enabling rapid mitigation of new threats.

About ReversingLabs

ReversingLabs is the trusted name in file and software security. We provide the modern cybersecurity platform to verify and deliver safe binaries. Trusted by the Fortune 500 and leading cybersecurity vendors, RL Spectra Core powers the software supply chain and file security insights, tracking over 422 billion searchable files with the ability to deconstruct full software binaries in seconds to minutes. Only ReversingLabs provides that final exam to determine whether a single file or full software binary presents a risk to your organization and your customers.

Get Started!

REQUEST A DEMO

reversinglabs.com

SB-Rev-10.29.25

REVERSINGLABS

Worldwide Sales: +1.617.250.7518
sales@reversinglabs.com