Securing Software Supply Chains in Fully Disconnected Federal Environments with Sonatype SAGE

SAGE packages Sonatype Lifecycle, SBOM Manager, Nexus Repository, and Nexus Firewall with SAGE Data Services, plus an optional Central Mirror—delivering policy decisions, component governance and SBOM intelligence entirely offline and kept current via signed, validated update bundles.

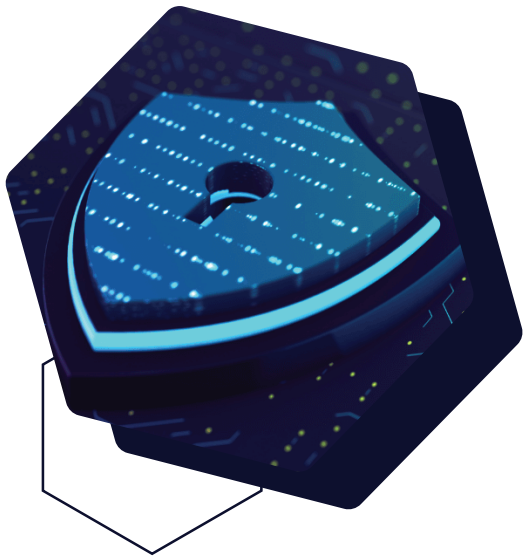
Technical Summary

In classified and air-gapped environments where internet connectivity is prohibited, Federal agencies face a critical challenge: how to maintain robust software supply chain security without external network access.

The Sonatype Air-Gapped Environment (SAGE) addresses this challenge by delivering comprehensive software supply chain intelligence and control entirely within disconnected networks. SAGE is a bundled solution that packages Sonatype Lifecycle, Nexus Repository, Software Bill of Materials (SBOM) Manager, Nexus Firewall and the SAGE Data Service, along with an optional Mirror of Maven Central, into a unified platform designed specifically for high-side operation.

With over a decade of experience serving Intelligence Community (IC) and defense customers, SAGE enables Federal agencies to enforce policy-as-code governance, generate and monitor SBOMs at scale and maintain continuous compliance with frameworks including National Institute of Standards and Technology (NIST) Secure Software Development Framework (SSDF), Executive Order (EO) 14028 and Cybersecurity and Infrastructure Security Agency (CISA) Binding Operational Directives (BOD) 22-01, all without requiring a single external network call.

By relocating the entire system inside the enclave, SAGE empowers development teams to maintain velocity while meeting the stringent security and accreditation requirements of the Department of Defense (DoD), IC and Federal civilian programs. Organizations can operate with the same level of software intelligence and artifact control available in connected environments, ensuring that mission-critical applications remain secure, compliant and resilient against emerging threats.



RESOURCES

Sonatype Air-Gapped Environment
carah.io/air-gapped-environment

Securing Air-Gapped Supply Chains
carah.io/sonatype-supply-chains

From Awareness to Assurance in Federal Software Development
carah.io/sonatype-software-development

CONTACT US

(888) 662-2724
Sonatype@carahsoft.com
carahsoft.com/sonatype

sonatype | carahsoft.

Securing Software Supply Chains in Fully Disconnected Federal Environments with Sonatype SAGE

How It Works

SAGE operates through a carefully architected low-side to high-side update workflow that maintains complete isolation while ensuring current intelligence. On the low-side (unclassified/connected) environment, designated systems retrieve signed intelligence bundles containing vulnerability data, license information and component metadata from Sonatype's cloud services. These bundles undergo cryptographic validation using Sonatype Update Tools before transfer. Once validated, the signed bundles traverse the approved cross-domain solution or guard mechanism into the high-side (classified/disconnected) environment.

Within the high-side enclave, SAGE Data Services ingests these validated bundles, providing local malware, vulnerability, license and component intelligence that powers all offline policy decisions and reporting. Initial deployments receive a full data load, while subsequent updates apply incrementally, typically daily, to keep intelligence current with little to no manual intervention. Organizations that successfully automate this process can complete the entire update cycle in a few hours during off-peak periods, allowing teams to start each day with the latest threat intelligence.

Sonatype Lifecycle supplies policy and metadata decisions directly to Continuous Integration / Continuous Deployment (CI/CD) pipelines and developer tooling, evaluating components against configurable policies including Key Exploited Vulnerability (KEV)-aware prioritization, license compliance and security risk thresholds. Nexus Repository serves as the trusted source for components and containers, providing role-based access, staging workflows, immutability and complete audit trails. The SBOM Manager maintains a central store for SBOMs, enabling offline generation directly from binaries and container images, critical when source code is unavailable.

For Java-heavy programs, the optional Central Mirror provides a point-in-time snapshot of Maven Central with regular updates. This enables high-throughput builds entirely within the enclave and eliminates the complexity of curating dependencies across the air gap.

SAGE requires external PostgreSQL databases for Lifecycle and Nexus Repository, runs on Red Hat Enterprise Linux (RHEL) 8/9 and deploys entirely within the high-side enclave. The architecture supports enterprise-scalable, highly available configurations through Kubernetes, enabling support for tens of thousands of developers.

Key Benefits

Complete Offline Operation with Federal Compliance

SAGE delivers comprehensive SBOM generation, policy enforcement and vulnerability management entirely on the high side with no external network calls. Policies and automated evidence collection support NIST SSDF, EO 14028, Office of Management and Budget (OMB) M-22-18/M-23-16 and CISA BOD 22-01 requirements, producing audit-ready artifacts for Risk Management Framework (RMF) and continuous Authority to Operate (cATO) processes without additional headcount.

SBOM Generation and Management at Scale

Generate SBOMs directly from binaries, container images and source code, addressing the challenge of compiled artifacts, Commercial Off-The-Shelf (COTS) software and legacy applications. Continuous monitoring re-evaluates SBOMs against new Common Vulnerabilities and Exposures (CVEs), KEV items and license changes, enabling true enterprise-scale SBOM management across polyglot environments, including containers, operating system (OS) packages, C/C++ and modern package managers.

Developer Productivity Without Compromise

Maintain developer velocity through Golden Versions recommendations, pull request comments, Integrated Development Environment (IDE) integration and automatic waivers where no fix exists. KEV-aware vulnerability prioritization ensures teams address actively exploited vulnerabilities first, while policy-as-code governance delivers consistent risk management across all builds and deployments.

Proven Maturity and Enterprise Scale

As the most mature air-gapped solution with over 10 years of serving IC and DoD customers, SAGE was purpose-built for classified environments. SAGE customers receive dedicated support from engineers with clearances who can operate on-site, while Kubernetes-based architectures scale to tens of thousands of developers. Centralized artifact management through Nexus Repository enables shared-service models that reduce duplication across programs within the same enclave.

sonatype | carahsoft