



CleanStart AI-SBOM

Complete Visibility Across Data, Models, and Dependencies

Ensuring data, model, and dependency integrity from build to production.



Executive Summary

AI is transforming enterprise software, but it is also introducing a new form of supply chain complexity.

Models, datasets, and frameworks evolve faster than traditional security tools can keep up. **CleanStart AI-SBOM** provides a unified, automated way to see and secure every layer of your AI system, from dataset lineage and model provenance to runtime dependencies.

It embeds verifiable metadata and cryptographic attestations during build, providing continuous visibility, compliance assurance, and operational trust throughout AI pipelines.

The Visibility Gap in AI Supply Chains

Modern AI stacks rely on layers of open-source frameworks, pretrained models, and external datasets.

Traditional SBOMs capture code dependencies but fail to account for AI-specific components such as data provenance, model lineage, and fine-tuning artifacts.

This visibility gap creates significant challenges for enterprises:

Opaque AI Dependencies: Model weights, adapters, and frameworks often originate from unverifiable sources.

Untracked Dataset Provenance: Data lineage and consent validation are rarely documented.

Fragmented Compliance: Current SBOM formats lack alignment with frameworks like NIST AI RMF or the EU AI Act.

Manual Evidence Collection: Security teams spend weeks generating documentation that quickly becomes outdated.

The CleanStart Solution

CleanStart AI-SBOM extends traditional SBOMs to deliver complete transparency for AI and ML systems. Built into **CleanStart Platform**, it automatically captures, signs, and validates all components of the AI supply chain.

Each build integrates:

Dataset Lineage: Provenance, licensing, and integrity of training data.

Model Metadata: Frameworks, adapters, weights, and fine-tuning sources.

Dependency Graphs: Verified open-source libraries and runtime components.

Cryptographic Attestations: Evidence stored immutably for audits and compliance checks.

CleanStart AI-SBOM transforms AI visibility from a manual documentation exercise into an automated, verifiable capability embedded within the infrastructure.

Key Capabilities



SPDX 3.0 AI Schema Integration

Captures data, model, and runtime artifacts in a verifiable format.



Dataset Provenance Tracking

Establishes cryptographic lineage for training and fine-tuning datasets.



Provenance Engine

Links model and dataset attestations through SLSA Level 4 build processes.



Hermetic Build Validation

Ensures reproducibility and isolation across training and deployment environments.



Automated Evidence Export

Generates signed attestations for NIST AI RMF, EU AI Act, and FedRAMP compliance.

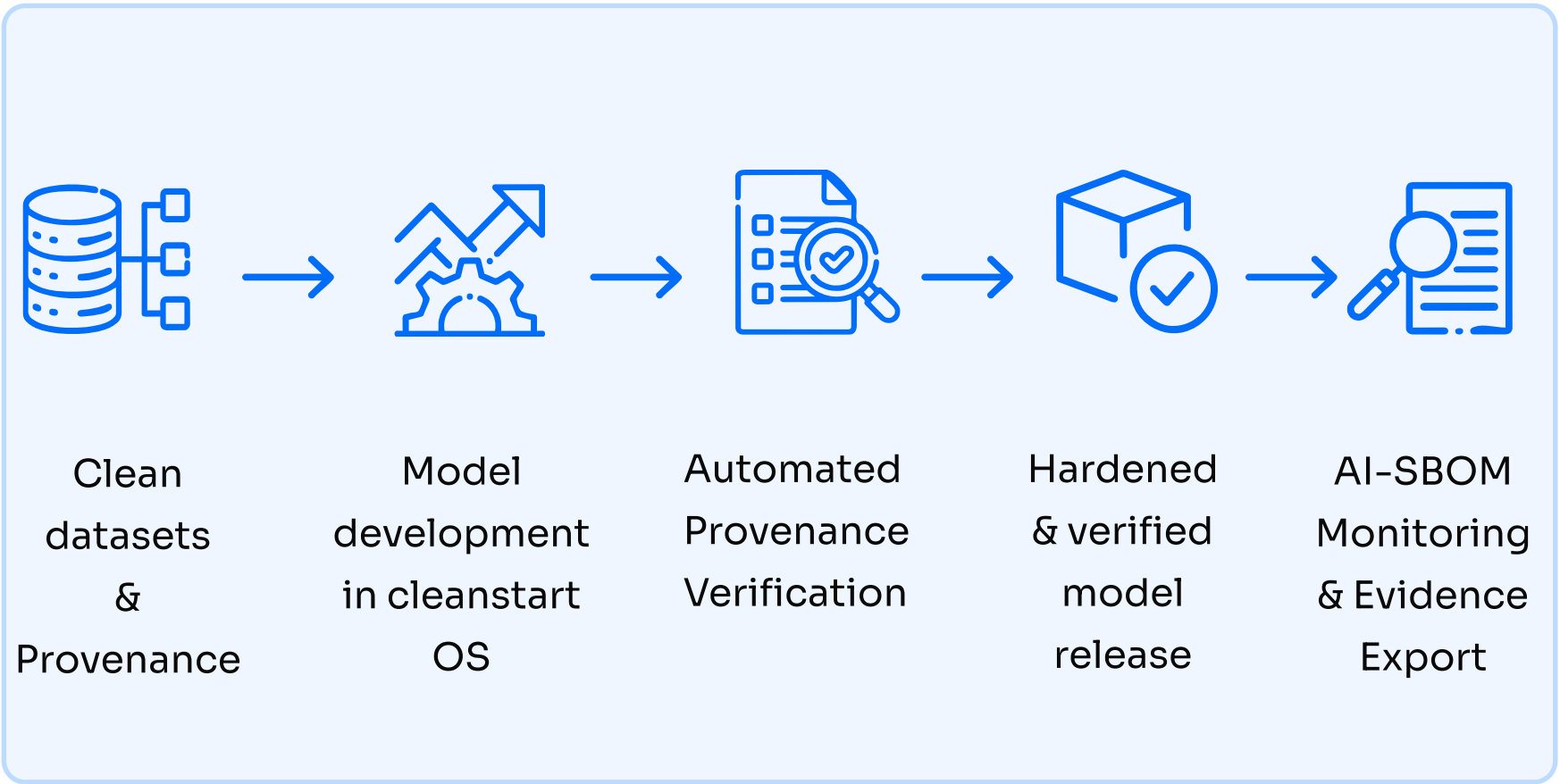


Runtime Visibility

Maintains live traceability of AI components in containerized inference pipelines.

CleanStart AI-SBOM Workflow

Visibility and assurance across the AI supply chain — from clean data ingestion to continuous compliance reporting.



Why CleanStart

Full-Stack Transparency: Unified view of data, model, and runtime dependencies.

Compliance by Design: Automated, audit-ready attestations.

Reduced AI Risk Exposure: Detects hidden model dependencies and dataset vulnerabilities.

Operational Efficiency: Cuts manual reporting and validation effort by up to 80 percent.

Future-Ready Framework: Built to evolve with emerging AI security and governance standards.

Integration and Availability

Integrates with: Kubernetes, GitHub Actions, OpenShift, TensorFlow, PyTorch

Supported Standards: SPDX 3.0, SLSA Level 4, NIST AI RMF 2024, EU AI Act 2025

References & Standards Alignment

CleanStart AI-SBOM aligns with the latest international standards and AI governance frameworks for software and model assurance:

SPDX 3.0 Specification (Linux Foundation, 2024): Defines AI-specific extensions for dataset and model metadata representation.

SLSA Framework (Level 4, 2025): Ensures reproducible and hermetically sealed build pipelines for artifact provenance.

NIST AI Risk Management Framework (2024): Supports transparency and accountability across AI lifecycle operations.

EU AI Act (2025): Provides compliance readiness for AI documentation and model governance.

FedRAMP Continuous Monitoring (ConMon): Enables continuous evidence generation for regulated deployments.

CleanStart Platform integrates these standards natively to deliver verifiable transparency and continuous compliance across AI supply chains.