Keysight SBOM Manager

Full-Lifecycle SBOM Visibility for Secure Software Supply Chain

Overview

Keysight SBOM Manager is a modular, enterprise-grade platform that delivers full-lifecycle Software Bill of Materials (SBOM) visibility, validation, and security intelligence. Built for both producers and consumers, it combines advanced binary-level SBOM generation with powerful SBOM validation, enrichment, sharing, and monitoring capabilities. Whether you're securing firmware, containers, software packages, or supplier-provided SBOMs, Keysight SBOM Manager ensures software supply chain confidence at scale.

Designed to address the unique needs of security, compliance, and engineering teams, Keysight SBOM Manager helps organizations proactively manage software risks across development, procurement, deployment, and post-market operations. It supports both first-party and third-party SBOM workflows, enabling teams to accurately detect components, verify and enrich SBOMs, continuously monitor for new vulnerabilities, and remain aligned with evolving regulatory requirements.

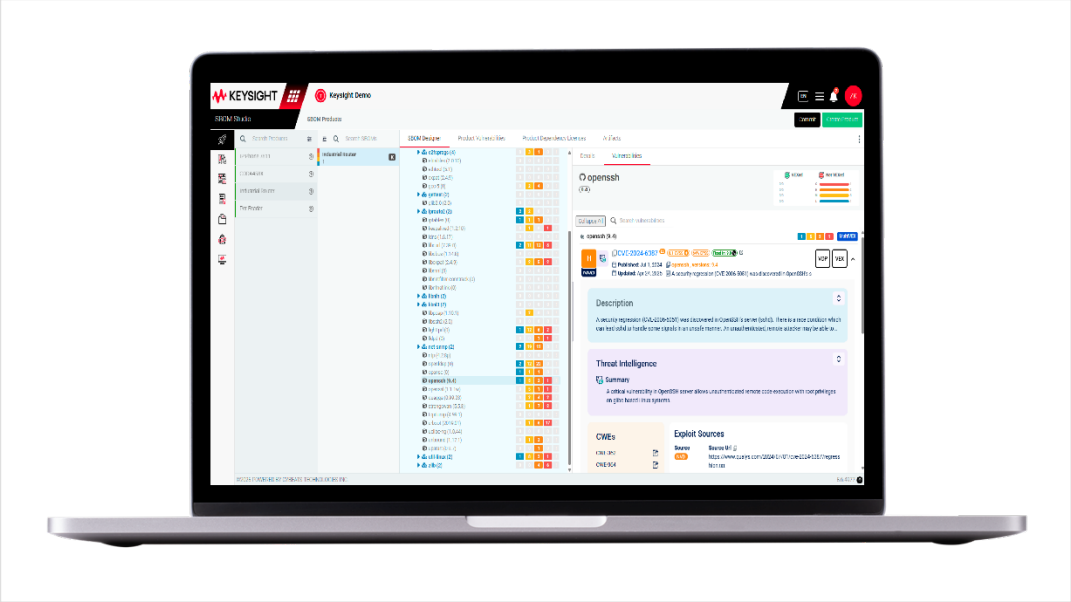

Figure 1. Keysight SBOM Manager

KEYSIGHT

Key Offerings

SBOM Generator

Keysight SBOM Generator is a next-generation binary analysis engine designed to extract highly accurate SBOMs from compiled binaries, firmware, containers, and VM images. It uses patent-pending binary similarity analysis and code emulation techniques to detect both open-source and proprietary components, without requiring source code or build access.

Capabilities:

- Extracts SBOMs from firmware, containers, and software binaries
- Detects open and closed source components
- Analyzes compressed firmware via high-speed unpacking
- Identifies components not declared in source-based SBOMs
- Supports legacy firmware
- Produces SPDX 2.3 and CycloneDX 1.6 compatible SBOMs
- Performs Automated Vulnerability Reachability Analysis and Generates VEX

Use Cases:

- Manufacturers needing visibility into legacy code
- Regulatory SBOM submissions without build access
- Validating vendor-provided SBOMs against actual binaries

SBOM Studio

SBOM Studio is the central hub for managing and operationalizing SBOMs. It enables full-lifecycle SBOM governance, from validation and enrichment to continuous vulnerability monitoring and regulatory compliance. Whether your SBOMs come from Keysight SBOM generator or third parties, SBOM Studio ingests, scores, enriches and monitors them.

Capabilities:

- Validates and auto-corrects SBOM format, structure, and completeness
- Enriches SBOMs with vulnerability and threat intelligence data
- Continuous monitoring via NVD, CISA KEV, GitHub, OSV, etc.
- Assigns SBOM Quality Scores based on coverage and accuracy
- Automates license analysis and GRC compliance reporting
- Dashboards for product, security, and compliance teams
- Integrates with CI/CD tools, ticketing systems, and SCA pipelines

Use Cases:

- Automating compliance with FDA, EU CRA, EO-14028, and Cert-In
- Prioritizing vulnerabilities using context-aware insights
- Enhancing DevSecOps with SBOM-driven workflows

SBOM Consumer

SBOM Consumer enables software and device buyers to validate and monitor SBOMs received from suppliers and vendors. It provides real-time threat visibility, SBOM structure validation, and ongoing vulnerability tracking, empowering buyers to trust the products they acquire and deploy.

Capabilities

- Imports and validates SBOMs from external vendors
- Continuously monitors components for newly disclosed threats
- Connects with asset and vulnerability management platforms
- Flags missing or malformed SBOM fields
- Automates third-party risk assessments
- Supports regulatory and contractual compliance workflows

Use Cases

- Ensuring security and compliance in procurement
- Monitoring deployed software for emerging CVEs
- Enhancing third-party software risk governance

Key Benefits

Table 1. Benefits

Benefit	Description
Enhanced security	Gain actionable visibility into components and vulnerabilities across all software types.
Accurate SBOM generation	Detect hidden, unreported, or unknown components through binary-first analysis.
SBOM quality validation	Improve the reliability of your SBOMs by detecting structural and semantic issues.
Regulatory compliance	Automate processes to meet requirements from FDA, EU CRA, ORAN WG11, and others.
CVE prioritization	Cut through CVE overload with context-aware enrichment and exploitability scoring.
Operational efficiency	Automate manual validation, licensing checks, and vulnerability monitoring.
Vendor SBOM monitoring	Continuously assess third-party SBOMs to ensure long-term software assurance.
SBOM lifecycle visibility	Centralized dashboards ensure collaboration across product, security, and procurement teams.

Who Uses Keysight SBOM Manager?

Device manufacturers and software vendors: Create secure, compliant software and firmware, even when legacy or third-party code lacks transparency.

Product buyers: Validate, monitor, and trust vendor SBOMs with ongoing threat intelligence and governance.

Service providers: Evaluate and secure third-party devices and software they deploy or resell.

Compliance and risk teams: Automate SBOM-related audits, license checks, and supply chain risk management.

Why Keysight SBOM Manager

Table 2. Keysight SBOM Manager vs typical SBOM tools

Feature	☑ Keysight SBOM Manager	☒ Typical SBOM Tools
SBOM generation approach	Binary-first analysis of shipped firmware, binaries, containers, and VM images	Mostly source / build-based
SBOM accuracy and coverage	High-fidelity detection of open-source, closed-source, legacy, and proprietary components	Limited to declared or OSS components with lower coverage
Detection of vendor / proprietary blobs	Yes	No
Component identification quality	High quality with CPE and PURL assignment	Inconsistent or missing identifiers
SBOM auto-correction and normalization	Automated validation, correction, and enrichment	Manual fixes required
SBOM quality scoring	Objective quality and completeness scoring	Limited or none
Vulnerability intelligence sources	NVD, EUVD, CISA KEV, OSV, GHSA, vendor advisories, more	Often NVD-only or limited sources
Continuous vulnerability monitoring	Near-Real-time, lifecycle-based monitoring	Periodic or manual refresh
VEX support at scale	Lifecycle-aligned, scalable VEX generation and management	None, limited or manual
Vulnerability triage	Context-aware CVE filtering and triage	CVE overload, no context
Vulnerability prioritization and notification	Policy-based	Limited or none
Centralized SBOM governance	Portfolio-wide dashboards and workflows, and version control	Limited or none
Secure SBOM and VEX sharing	Role-based access, controlled distribution, traceability	Manual sharing (email / files)
Integration with asset discovery solution	Maps SBOMs to deployed assets and versions	None
Compliance-ready reports	EU CRA, FDA, Cert-In ready	Limited or ad hoc

Audit trails and evidence generation	Regulator-ready audit artifacts	Manual documentation
Multi-BOM support	SBOM, HBOM, AIBOM, CBOM	SBOM only
Multi-tenancy support	Full multi-tenant architecture with strict data isolation across organizations	Typically single-tenant or weak logical separation
Cross-tenant governance	Centralized governor dashboard to manage all tenants, and data from a single interface	No unified cross-tenant governance
User scalability model	Unlimited users without per-seat constraints	Per-user licensing or scalability limitations
DevOps ecosystem integration	Native integrations with CI/CD, Jenkins, GitHub Actions, Jira, and Identity Providers	Limited, fragmented, or custom integrations required
API-first automation	Comprehensive REST APIs enabling full automation and integration into existing workflows	Partial or limited API coverage
End-to-end workflow orchestration	Integrated workflows spanning SBOM ingestion, analysis, triage, and reporting across teams	Disconnected tooling with manual handoffs

Ordering Information

983-1501

SBOM Manager License for SBOM Studio Module for a Single Licensed Studio SBOM (1-year subscription, floating worldwide license). Min 20 units per order.

983-1502

SBOM Manager License for SBOM Studio/Consumer Module for a Single Tenant Addon (optional license) (1-year subscription, floating worldwide license)

983-1503

SBOM Manager License for SBOM Studio/Consumer Module, Optional Addon for Governor Dashboard Tenants (1-year subscription, floating worldwide license)

983-1504

SBOM Manager License for SBOM Generation Module per single scan. Min 30 units per order. (1-year subscription, floating license). TAA compliant

983-1505

SBOM Manager License for SBOM Consumer Module for a Single Licensed Consumer SBOM (1-year subscription, floating worldwide license). Min 20 units per order.

Proposed Ordering Options

For Device Manufacturers and Software Vendors:

- 983-1501: SBOM Manager License for SBOM Studio Module for a Single Licensed Studio SBOM
- 983-1504: SBOM Manager License for SBOM Generation Module per Single Scan

If additional tenants are needed:

- 983-1502: SBOM Manager License for SBOM Studio/Consumer Module for a Single Tenant Addon
- 983-1503: SBOM Manager License for SBOM Studio/Consumer Module, Optional Addon for Governor Dashboard Tenants

For Service Providers, Enterprise Deployers, and Consumers

- 983-1505: SBOM Manager License for SBOM Consumer Module for a Single Licensed Consumer SBOM
- 983-1504: SBOM Manager License for SBOM Generation Module per Single Scan

If additional tenants are needed:

- 983-1502: SBOM Manager License for SBOM Studio/Consumer Module for a Single Tenant Addon
- 983-1503: SBOM Manager License for SBOM Studio/Consumer Module, Optional Addon for Governor Dashboard Tenants