

# SBOM Insights

## Gain Intelligence with a SaaS Solution for SBOM Management

### Why the Software Supply Chain Matters

Modern software creation stretches beyond the walls of a specific developer or software engineering team. A single application includes various parts, multiple developers, partners, and systems from both inside and outside an organization, very similar to the production of a commercial airplane. Just like in manufacturing a piece of hardware, all of the components are most likely not proprietary. Audit data shows that 80 percent of the software scanned does not originate from the vendor whose code is being scanned. However, once that software is shipped to customers or downstream supply chain partners, as the owner/distributor, you are responsible. By virtue of consumption, you take on the legal risk of potential vulnerabilities and compliance issues within that code. Tracking those components, knowing where they exist in an application and from where they originated has become a priority for both software creators and consumers. Why? Because the software industry is immensely reliant on open source software and third-party code, creating an inflection point.

The use of open source is on the rise, as well as the increase in the number of dependencies found in codebases, mostly based on the number of programming languages in play. Vulnerabilities are going up and security exploits are increasing exponentially, beyond the ability for manual intervention and management. Furthermore, regulations such as the U.S. Cybersecurity Executive Order requiring more focused management and intelligence around the use of open source software creates a perfect storm for the software supply chain.

### KEY FACTS:

- Manage a complete Software Bill of Materials (SBOM) in a SaaS environment
- Ingest data from a wide range of sources, unifying internal and external SBOMs across your organization into a single actionable view
- Generation of compliance artifacts for customers and downstream supply chain partners

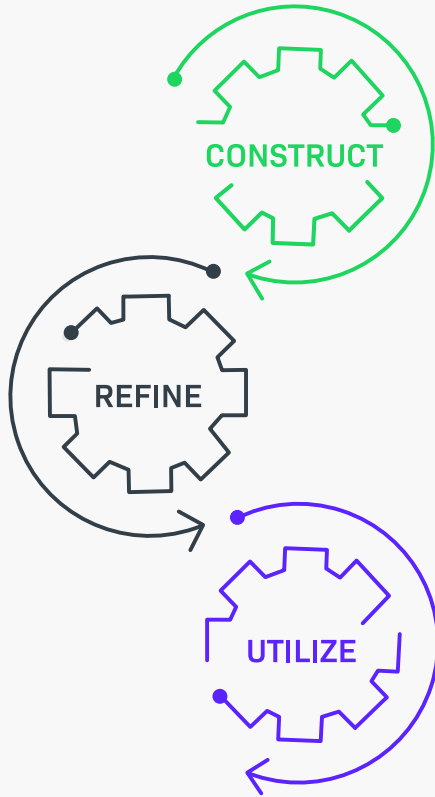
### INSIGHT



*Over 2,200 SBOM parts were discovered as part of an average software application audit. In some cases, the number of parts exceeded 10,000—an increase of 12% from the prior year. This in many cases represents the vast majority of software elements within a commercial application; often exceeding 80% of the lines of code.*

*—2022 Report on Software Supply Chain Compliance*

## THE SBOM LIFECYCLE



### CONSTRUCT

Your SBOMs representing your portfolio of applications consist of parts that come from many different places, both inside and out of your organization. This phase takes all that SBOM data—including open source components, third-party code, and commercial—reconciles it, and presents it in an actionable unified view.

### REFINE

Because the data is coming from multiple sources, there are varying levels of quality. There may be gaps to fill, issues to resolve, and needed adjustments to further refine your SBOMs before publishing them for internal and external consumption.

### UTILIZE

Now that your SBOM source of truth is catalogued, fulfill obligations and assess your security and compliance risk with confidence. Generate compliance artifacts, view usage insights and trends, and perform impact analysis—as new vulnerabilities are discovered—to allow your development, security, and legal teams make better decisions for your business.

The ability to scan and discover what's in your code and then create a software bill of materials (SBOM) is only part of the story to identifying open source and third-party components in your applications. You need a solution that collects information from all corners of your organization, as well as from upstream supply chain partners, aggregates that data into a single repository, and provides full visibility for security, legal, and downstream supply chain partners to act on the results.

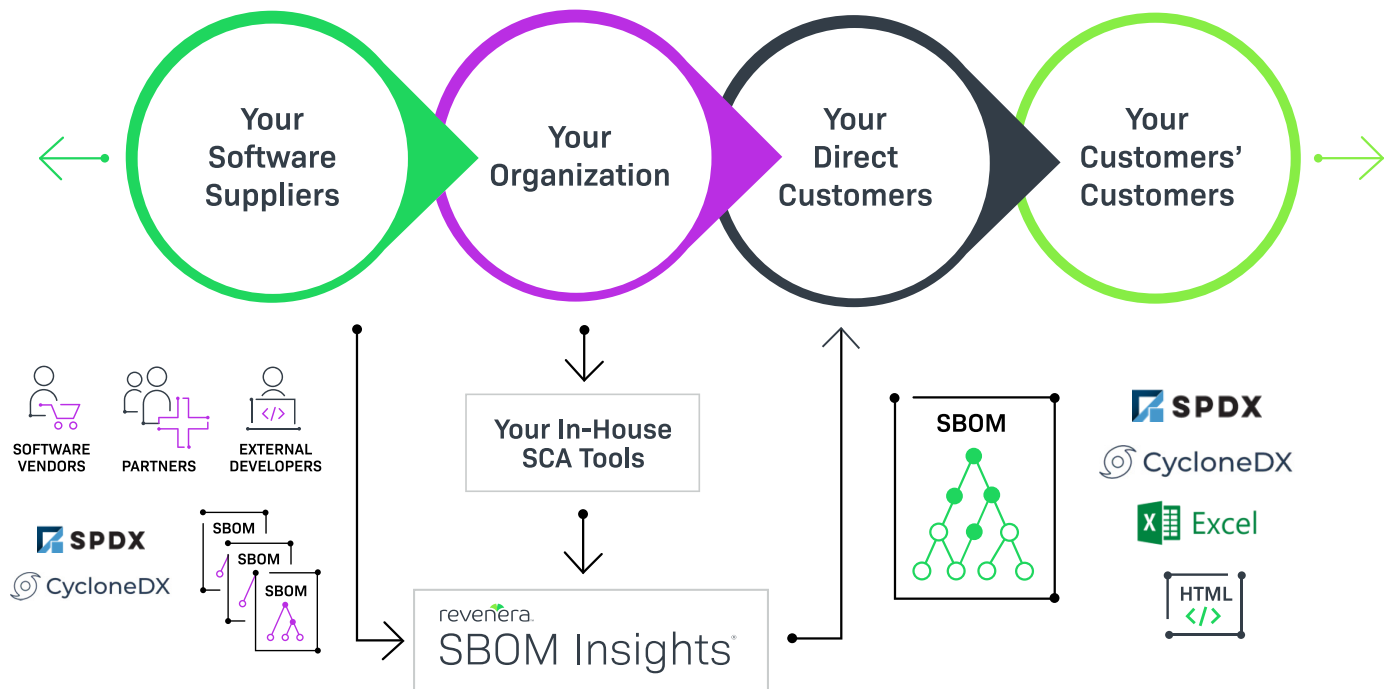
Reverera SBOM Insights gives you the ability to manage security and legal risk by maintaining an actionable SBOM in a SaaS environment for more supply chain control and transparency.

## Increase Transparency in Your Software Supply Chain

With SBOM Insights, you not only have the ability to identify and record all the parts in your applications through a complete and accurate SBOM, but to collect your SBOM parts from multiple sources—in various industry formats.

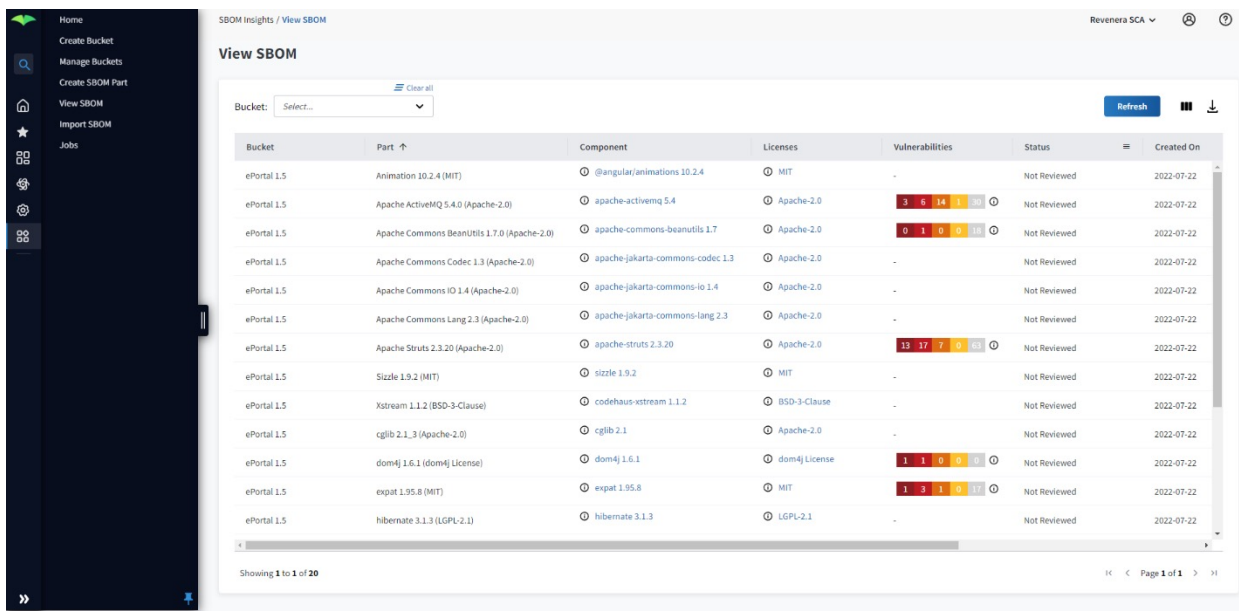
SBOM Insights creates an active repository—with actionable data—of what's in your applications.

### THE SOFTWARE SUPPLY CHAIN AND SBOM MANAGEMENT WITH SBOM INSIGHTS



SBOM Insights goes beyond being a document storage system. It enables you to ingest SBOM data from partners, vendors and suppliers in SPDX and CycloneDX formats, reconcile and normalize the data for a unified view. Furthermore, this advanced technology provides you with insights into the components you use. Identify outdated components, security vulnerabilities, and open source license compliance issues.

With everything coming from your enterprise catalogued, when the next high-profile vulnerability hits, you have the unified data at your fingertips to quickly uncover your exposure and expediently fix problems—not just in the code you scanned, but also in all of the software components coming from outside your organization.



With SBOM Insights, you can::

- Unify all SBOMs into single, actionable view in the cloud
- Ingest data from a wide range of data sources—both inside and outside of your organization
- Give full open source and third-party component visibility to legal teams, security, and supply chain partners

## Analyze and Act on Your SBOMs with Intelligence

SBOM Insights supports the ingestion, reconciliation, aggregation, and visibility of all SBOMs in order to provide the needed insights to manage legal and security risk, deliver compliance artifacts, and secure the software supply chain:

- Enhance your software development operations with increased transparency
- Aggregate and reconcile SBOMs from multiple data sources
- Control license compliance and security risk

### NEXT STEPS

Gain transparency and actionable insights into the complexity of your software.

[LEARN MORE >](#)

Reverera provides the enabling technology to take products to market fast, unlock the value of your IP and accelerate revenue growth—from the edge to the cloud. [www.reverera.com](http://www.reverera.com)