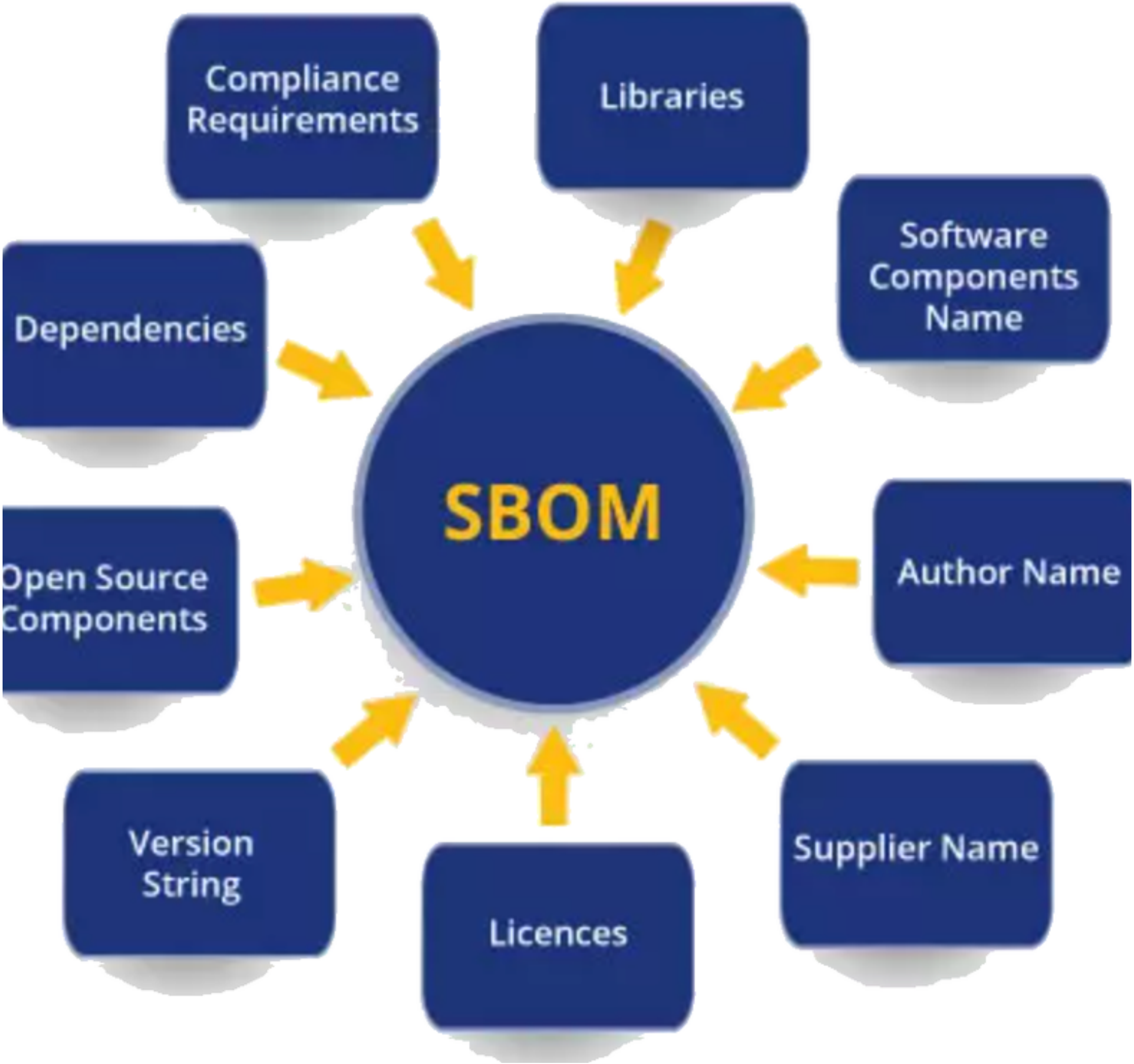
# Software Bill of Materials

Jennifer Morales (C)
Contingent Worker



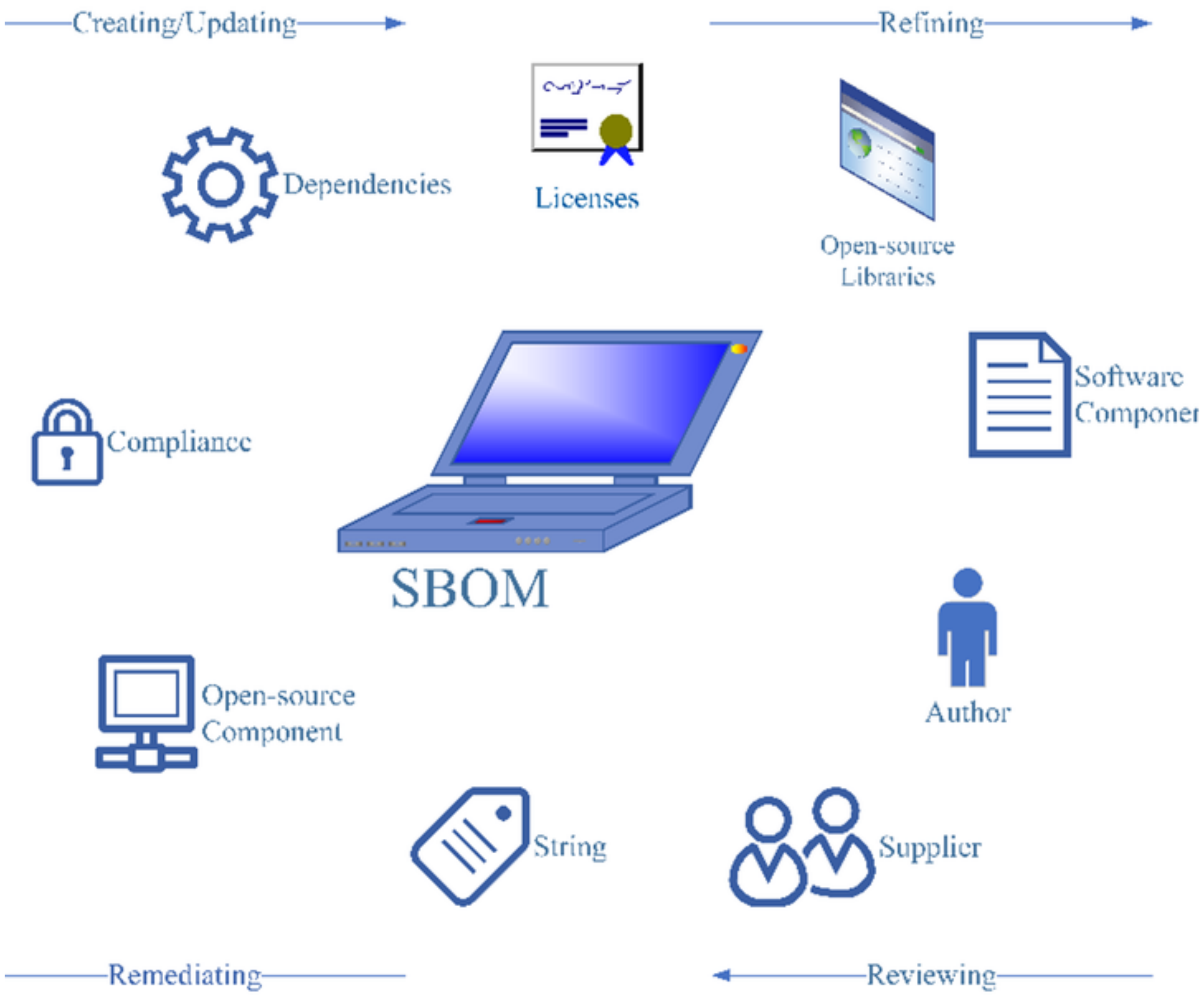
## Software Bill of Materials Definition

Owing to the ever-changing technological capabilities, there has been an exponential increase in the instances of cyberattacks worldwide. In order to cope with such malicious events, cyber experts are constantly involved in developing counter approaches. One of these frameworks is the creation of a document, namely a software bill of materials (SBOM). According to Janet Worthington, a senior analyst at Forrester, an SBOM is capable of providing visibility into the quality, security, and license compliance of the software. Given Vertex' primary mission of reducing the friction of commerce and the need to withstand cyber-threats, the SBOM is a vital tool in any software-chef's kitchen.

An SBOM is essentially a list of ingredients for software. Thus, an SBOM can be defined as a machine-readable inventory of all open-source and third-party software components, and open-source licenses as well as dependencies existent in a codebase. As per Ed Moyle, a systems and software security director at Drake Software, an SBOM is a list containing software components and dependencies in a specified product. Therefore, the design of an SBOM is aimed at tracking the specificities and relationships in the supply chain of software components, thereby, providing transparency directed at fixing cyberthreats. The SolarWinds supply chain attack is one such case in point prompting President Joe Biden to promulgate the Cybersecurity Executive Order, 2021.

## Working of an SBOM

An SBOM can be generated using software composition analysis tools, such as FOSSA and Black Duck. In accordance with the minimum standards and requirements issued under the Biden Administration's Executive Order and publicized by the National Institute of Standards and Technology (NIST), an SBOM works on the principle encompassing three key domains, namely, data fields, automation support, and practices and processes.



- Data Fields: Tasked with enumerating rudimentary data related to software components, i.e., the name of the supplier and component, its version, dependency, unique identifiers, and SBOM author along with the timestamp, data fields are the essential elements concerned with the operation of an SBOM.
- Automation Support: An SBOM is necessarily based on machine-readable formats, i.e., CycloneDX, Software Package Data Exchange (SPDX), Software Identification Tags. Ed Moyle has rightly said that manual tracking of dependencies is a massive job.
- Practices and Processes: The function of this element in an SBOM is concerned with the deployment particularly related to its distribution, identification of

undiscovered components, and their constructive management.

## Advantageous Features of an SBOM w.r.t. Businesses

An SBOM has relatively eased business processes including risk assessment, compliance due diligence, and tracking vulnerabilities. Some of the most desirable characteristics are mentioned below.

### *Efficient, Cost-effective, and Time-saving*

An SBOM has the capacity of significantly enhancing effective software administration by providing experts with a resourceful and low-cost solution, thereby, mitigating the need of manual, tedious, and time-consuming tasks.

### *Secure and Reliable*

To safeguard an organization against imminent cyberattacks, utilizing an SBOM effectively assists in evading as well as eliminating recognized threats through facilitating the process of due diligence.

### *Significant Supply Chain Resilience*

Businesses and institutions incorporating a controlled platform are often prone to unknown vulnerabilities. With the help of an SBOM, such malicious activities are surfaced prior to the breach, thus, improving the quality of the software as a supply chain.

### *Better Compliance*

As per the findings of the 2022 Open Source Security Risk and Analysis report, approximately 97 percent of the scanned codebases contain open-source components. Because of the open-source software availability, an SBOM provides a preferable medium of keeping records concerning software audit reviews and regulatory standards. In this way, compliance risks or licensing conflicts are smartly addressed.

## Market Trends

In response to investigating the 2021 security infringements in connection with Kaseya, Codecov, Apache Log4j, and SolarWinds, the Biden administration-issued Executive

Order has detailed recommendations directing firms and enterprises to corroborate safety and security related to software-based production by making use of an SBOM. In line with the new and established rules and regulations, the market is maturely employing SBOM in projects falling under the following categories:

- Fundraising, M & A, and IPO: Associated with mergers and acquisitions (M & A), initial public offering (IPO), and fundraising, an SBOM is a crucial constituent of technical due diligence. Concerned participants in the market effectuate software-based documentation pertinent to the products complying with the set standards.
- Regulatory Compliance: In conformity to the regulations stipulated in the Biden-issued Executive Order concerning supply chain security, business corporations are pragmatically publishing SBOM relevant to each and every product.
- Backward Compatibility: A backward compatible system is interoperable with an old legacy system. Business organizations maintaining old software utilize downward compatible feature via updating and upgrading the open-source software package in order to execute old data and information successfully.
- Preventing Software Supply Chain Attacks: Aimed at targeting software developers, supply chain attacks infect legitimate software applications throughout the globe. Therefore, as a prevention strategy, markets are productively implementing SBOM as part and parcel of their business processes.

The use of SBOMs is well beyond the Early Adopter phase and is headed to mainstream maturity. As noted by Stephen Hendrick, vice president of Research of The Linux Foundation, “I was surprised to find that 47% of organizations produced or consumed SBOMs in 2021. In many cases, this meant using SBOMs in a few or some segments of their business. But a surprising number of organizations were using SBOMs across nearly all of their business segments or had implemented SBOMS as an organizational standard. It was also exciting to see that *(an additional)* 41% of organizations plan to use SBOMs beginning in 2022 or 2023”.

## SBOM Providers

A list of top 10 SBOM providers along with the product description is outlined below.

1. WhiteSource SBOM: Focusing on open-source code, WhiteSource is one of the topmost SBOM providers aimed at identifying open-source packages, tracking each and every element, and remediating vulnerabilities.
2. Black Duck by Synopsys: In compliance with the NIST guidelines, Black Duck helps secure software supply chain through an updated version of SBOM capable of

generating SPDX 2.2 format.

3. FOSSA: Following a step-by-step methodology, FOSSA provides its users with a first-rate solution that is able to safeguard open-source supply chain.
4. JupiterOne: Another leading SBOM provider in the list is JupiterOne which generates SBOM based on CycloneDX format.
5. Methodics IPLM by Perforce: One of the top-tier providers of IP life cycle management and SBOM solutions, Methodics IPLM has the capacity of tracking the bill throughout the configuration.
6. Blackberry Jarvis 2.0: It is a software composition analysis solution that is positioned at listing as well as detecting open-source software in addition to tackling impending cyber vulnerabilities.
7. Snyk: Snyk is a cybersecurity platform that automates the entire process of SBOM workflow, thereby, expediting the overall mechanism.
8. Dependency-Track: Focused at mitigating supply chain threats, Dependency-Track builds a CycloneDX-based SBOM followed by producing a detailed analysis for security purposes and a real-time solution.
9. Ubuntu by Linux: Ubuntu is an open-source service provider that helps create an effective SBOM via its wide-ranging libraries.
10. Syft by GitHub: Last but not least, Syft is a command line interface (CLI) provider that helps generate an SBOM.
11. And a bonus - the product used by Vertex: Checkmarx SCA™ allows your developers to build software with confidence using a mix of custom and open source code.

## Conclusion

In view of the criticality of knowing what software is deployed and tracking the vulnerabilities and fixes for each component, an SBOM for digital infrastructure is an optimal policy. Whether you are running your own copy of software for corporate use or are consuming a SaaS-provided service, the ever-changing dependencies in the digital market and the emerging cyberthreats make incorporating state-of-the-art SBOM into businesses and organizations a necessity to maintain rapid growth.

Source articles for this page:

- Janet Worthington

- https://www.linkedin.com/in/edmoyle?original_referer=
- https://www.drakesoftware.com
- The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal
- Executive Order 14028, Improving the Nation's Cybersecurity .
- FOSSA: Audit-Grade Open Source Dependency Protection
- Black Duck Software Composition Analysis (SCA) | Synopsys
- OWASP CycloneDX Software Bill of Materials (SBOM) Standard
- International Open Standard (ISO/IEC 5962:2021) - Software Package Data Exchange (SPDX)
- Software Identification (SWID) Tagging | CSRC | CSRC
- Ed Moyle - Drake Software, Systems and Software Security Director
- [Analyst Report] 2022 Open Source Security and Analysis Report | Synopsys
- Kaseya VSA ransomware attack
- Codecov hackers breached hundreds of restricted customer sites - sources
- FTC warns companies to remediate Log4j security vulnerability
- https://www.linuxfoundation.org/blog/software-bill-of-materials-sbom-and-cybersecurity-is-your-organization-ready/
- Should companies ask for a SaaS software bill of materials? | TechT...
- https://www.linuxfoundation.org/blog/software-bill-of-materials-sbom-and-cybersecurity-is-your-organization-ready/

Add label