EBOOK

Business Drivers of SBOM Adoption

ABSTRACT

The Software Bill of Materials (SBOM), a detailed list of open-source, third-party, and commercial components used in a piece of software, enables software-producing organizations to provide transparency to customers and downstream supply chain partners by disclosing the composition of their applications to support better management of licensing and security risk within their applications. This ebook examines the nature of the SBOM, its business drivers, and how SBOM best practices have evolved in recent years.

Introduction

The practice of using open-source components and packages creates security risks and establishes licensing agreements with an expansive group of people, communities and entities. The Software Bill of Materials (SBOM), a detailed list of open-source, third-party, and commercial components, and any related licensing terms, enables a software maker to understand the composition of its software and ensure that it is complying with all relevant licenses and not passing potential risk to downstream users. The SBOM is much more than just a technical document, however. Done right, the SBOM delivers a range of business benefits, including the potential to make operations more efficient and improve customer relationships.

SBOM Overview

An SBOM is a complete, structured list of components used in the creation of a piece of software. It includes libraries and modules that are compiled and linked into the software. The SBOM shows the supply chain relationships between these components. The SBOM can consist of a combination of open-source, third-party, and commercial components. These components can be free or paid for, widely available or subject to restricted access.

DEFINITION

Software Bill of Materials (SBOM)

A SBOM is a formal and queryable record containing the details and relationships of various components used in building software.

Per the National Telecommunications and Information Administration (NTIA)

SBOMs exist for a number of reasons. Concerns about application security make stakeholders want to know what is inside the software that their organizations use. Malicious actors may inject malware into open-source libraries, spreading vulnerability throughout the software supply chain as infected components get built into software applications. With an SBOM, security analysts, the legal department, and development teams can search for known threats that might be present in their software. Cataloging the components across an organizations' portfolio of applications allows impact assessment for newly reported security vulnerabilities to drive remediation work and releases of patches to customers.

Businesses and public sector organizations also create SBOMs so they can stay on top of the varied licensing agreements that arise with the use of open-source components. Open-source software (OSS) components may be free, but they are not without contractual commitments or obligations. The SBOM helps organizations understand which components comprise their products to assist with maintaining compliance with the incurred legal obligations.

In some cases, software subject to government regulations or procurement policies must show an SBOM in order to be deemed compliant. These sorts of rules are proliferating, most recently through a Cybersecurity Executive Order from the U.S. Government that requires the Department of Commerce to publish standards for SBOMs for government software procurement processes.

Another example of government policies driving the use of SBOMs is H.R. 4611, the DHS Software Supply Chain Risk Management Act of 2021. This proposed law would require selected government contractors to submit an SBOM to the Department of Homeland Security (DHS) that provides, in its words, "a certification that each item in the bill of materials is free from certain security vulnerabilities or defects affecting the security of the end product or service, a notification of any identified vulnerability or defect, and a plan to mitigate, repair, or resolve any identified vulnerability or defect."

Regulated businesses are also often expected to produce SBOMs as part of their compliance programs. The FDA requires SBOMs in the healthcare industry. The National Highway Transportation and Safety Administration (NHTSA) mandates SBOMs from automakers. The Federal Trade Commission (FTC) insists on SBOMs in certain consumer industry contexts. The North American Electric Reliability Corporation (NERC) needs SBOMs in cases involving critical energy infrastructure. The European Union (EU) similarly requires SBOMs in use cases ranging from cloud computing, Internet of Things (IoT), telecommunications, healthcare, and payment cards.

INSIGHT

The software industry's reliance on ***open source****, along with a sharp increase in* ***dependencies****, and the frequency of* ***security exploits****, has set up a perfect storm for* ***supply chain security****.*

There are two ways to create an SBOM. In the past, people relied on manual processes, often resorting to spreadsheets to keep track of application components. However, as the volume of external code within an average application continued to increase, this approach became untenable. Others utilize a software composition analysis (SCA) tool that scans the code and generates the basis for an SBOM through a semi-automated process.

The SCA approach still has its limitations, especially when attempting to integrate multiple SBOMs from multiple scan tools, which is a common situation. Add to that the need to integrate upstream software suppliers and it can be quite difficult to obtain a single cohesive view of a product's ingredients.

Business Drivers of SBOM Adoption

Business drivers for SBOM adoption fall into three broad categories: risk management, efficiency, and building stronger partner and customer relationships. When properly executed, these categories translate into positive financial outcomes, either by cutting costs, reducing financial risk exposure or growing revenue.

In terms of risk management, the SBOM is an essential element of mitigating cyber threats. Having an SBOM enables security professionals to know where they can find malicious code in an application that the organization has built or purchased. The SBOM aids in responding to software supply chain attacks by pinpointing which applications across the enterprise need to be remediated to address the security issues.

INSIGHT

"By 2025, 60% of organizations building or procuring critical infrastructure software will mandate and standardize software bills of materials (SBOMs) in their software engineering practice, up from less than 20% in 2022."

GARTNER, HYPE CYCLE FOR OPEN-SOURCE SOFTWARE, JULY 2022

This is as much about business as technology. A data breach or major cyber incident resulting from a software supply chain attack can cost millions of dollars to remediate. According to the most recent IBM/Ponemon Institute report, the average cost of a breach is $4.24 million. Such an event will also result in brand damage and distraction from core business activities.

INSIGHT

$4.24 Million

The average cost of a data breach

IBM/PONEMON INSTITUTE REPORT, 2022

The SBOM also helps an organization manage risk related to legal liability and compliance. Use of software, both commercial and open-source, is subject to software license agreements. The organization using the software components is responsible for abiding by the terms of those licenses. Failing to do so creates legal liability, which can be expensive to handle due to forced remediation activities in released applications or injunctive measures impacting an organizations ability to sell their software. The SBOM provides a source of truth for components in use across an organization. This allows tracking of the resulting license obligations to remain compliant with their corporate OSS policies.

SBOMs are increasingly becoming part of the compliance landscape. Companies that work with military contractors, for example, are required to submit an SBOM with their software as part of the procurement and certification processes. The SBOM keeps the company in compliance with such rules, and thus keeps them in business with clients who need SBOMs.

The SBOM can be a driver of operational efficiency if it's produced using appropriate automated tools. It reduces time that software developers spend remediating out-of-compliance open-source code. This makes the open-source management team more productive. An SBOM can also contribute to faster dev/test (DevOps) cycles, reducing remediation for issues caught early in the dev cycle, which helps with time to market, keeping software projects on budget.

Other areas of the business benefit from the SBOM as well. For example, with an SBOM, the General Counsel's office can be more productive in staying on top of license usage and policies, and reviewing license compliance issues, and responding to problems that arise in the normal course of business.

INSIGHT

2300

Average number of open-source items discovered per audit project.

↑15% YOY

REVENERA AUDIT SERVICES, 2021

SBOMS
ARE GETTING LARGER, MORE COMPLEX, AND MORE DIFFICULT TO MANAGE.

SBOMs are also quite useful in the merger and acquisition (M&A) process—reducing time spent analyzing software owned or built by an acquisition target, while also minimizing inherited security or licensing issues that might arise after an M&A deal has closed.

On a related front, having an SBOM assists with complying with the attribution requirement in most open source licenses by preparing a third-party notices report based on the cataloged SBOM parts. Preparation of the attribution reports is still a necessary step as most SBOMs do not yet contain the necessary elements to satisfy this requirement, e.g., missing copyright statements and the actual license text. It also streamlines compliance with government regulations, which often takes a lot of people-hours to perform.

Having a thorough and well-organized SBOM should contribute to improved customer relationships, especially in today's environment when it's a competitive advantage to create trust in a software developer's reputation. More than ever before organizations are asking for a software inventory before engaging with a software vendor. The SBOM should also enhance relationships with downstream supply chain partners. The organization's standing with the open-source community will also likely get better when all stakeholders can access a complete SBOM that is regularly maintained over time. The process accrues to the organization's brand as a trusted source of software.

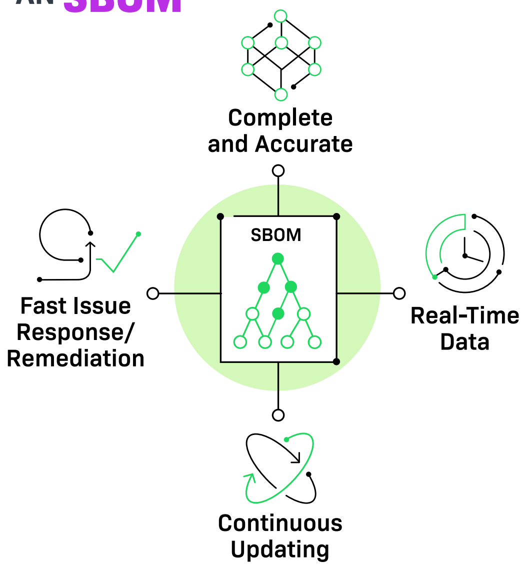
What These Business Drivers Mean for the SBOM

The forces pushing organizations to create SBOMs also exert some pressure to be more rigorous in the process. It's time to go beyond the common, but understandable mindset of, "We built an SBOM and handed it to someone." A new generation of SBOMs is arriving, in which the SBOM and its surrounded processes need to embody the following qualities:

- **Greater completeness and accuracy**—SBOMs are seldom 100% perfect, but it is highly preferable today for an SBOM to be as complete and accurate as possible. This means including all relevant components in a piece of software including all subcomponents, direct and resolved transitive dependencies, and associated licenses, coupled with as much supporting detail as is available, including the relationships between SBOM parts which indicate their provenance.

INSIGHT

QUALITIES OF AN SBOM



- **Ability to know what's being used in real time**—Stakeholders interact with the SBOM, so ideally the SBOM should enable people to know what is being used in a piece of software in real time. For example, if an open-source library was added to an application on the first of June, a legal analyst should be able to query the updated SBOM soon thereafter and see that library listed.
- **Regular, continuous updating**—Software is not static, especially in today's world of DevOps and continuous integration/continuous deployment (CI/CD). For this reason, the best practice is to update the SBOM regularly; ideally as an automated step in the CI/CD process.
- **Reactive capabilities**—The SBOM should help expedite reactions to security and license compliance issues within software applications. This might mean facilitating a rapid response to a threat that's detected in the code or helping to remediate a license issue once detected.

Selected SBOM Best Practices

SBOM best practices are evolving, and specific practices will vary by organization. The size of the organization, its business model and maturity will affect how it defines and adopts best practices. However, it is worth the effort to take a general look at current best practices because of the increasing importance of SBOMs for security, business and IT. The baseline assumption should be that manual, one-off approaches to SBOM creation are no longer adequate.

Automation

Automating SBOM creation is a best practice that makes it possible to keep SBOMs up to date. It should not be left up to security or software deployment teams to make time for manual production of SBOMs. Development and deployment teams are busy and under pressure to get solutions out to market as quickly as possible. They don't want stop their work and undertake manual efforts to locate and remediate issues. Their natural reaction is to put off the task until their schedules open up.

Automation alleviates many of these problems by taking the bulk of the SBOM prep work out of the hands of team members. It also makes the SBOM vulnerable to loss of knowledge that occurs when people quit or change jobs.

Automation does have its limits, though, and will always have coverage gaps. Deeper scanning and manual analysis is often required to further refine the SBOM with items beyond monolithic libraries—covering components like individual files, code fragments, and non-code file such as multimedia, images, icons, and documents.

The Frequency of SBOM Preparation

How often should an organization update its SBOM? This is partly a matter of practicalities. SBOMs take work, even when they are automated. There is going to be some time interval elapsing between SBOM refreshes. It's not realistic to plan a new SBOM update every day, though remarkably it is possible to do this if necessary—a "live view" based on a continuous automated SBOM process.

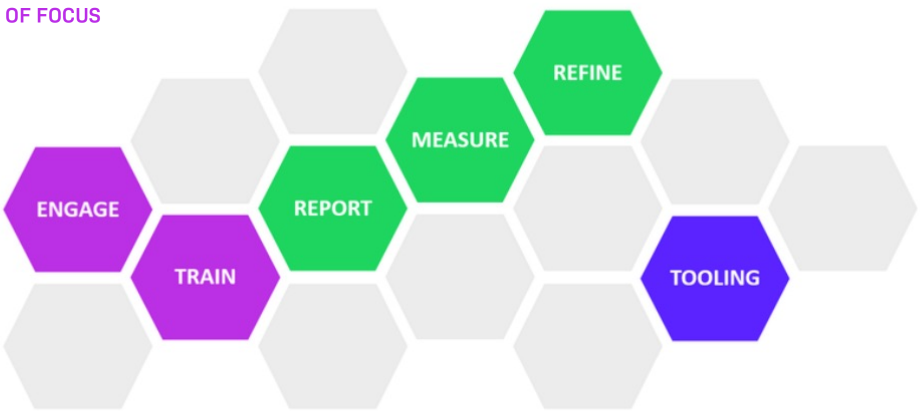
The answer depends partly on context. A software-as-a-service (SaaS) application that is frequently updated will do better with more frequent SBOM updates than an on-premises application on a scheduled release cycle. Waiting until the moment of product release is generally considered too late. For a SaaS app, there should be a regular cadence of SBOM updating that the team can realistically support, such as once a month.

The best practice is to update your software inventory as often as it makes sense. This might mean doing it at regular intervals or upon the release of new code. Some organizations update SBOMs based on code changes. It is also wise to think through how often recipients of the SBOM can realistically handle receiving an update. What will they do with a new SBOM data set? How extensive should that data set be? Given the inevitable constraints on everyone's time, an incremental approach may be best.

OSPO

Organizations that use open-source components in their applications do well by establishing some form of an Open-Source Program Office (OSPO). Again, the scope and sophistication of such an effort will depend on the size and complexity of the organization and its software projects, but the best practice is the same: An OSPO exists to organize and coordinate open-source program activity in an organization. Team members participating the OSPO develop and maintain policies for using OSS. When set up this way, the OSPO becomes the first call—and last word—on any open-source activity. The OSPO further serves as a point of engagement with the broader open-source community.

OSPO AREAS OF FOCUS



An OSPO may also take on certain technical functions, often performed jointly with the engineering team. For instance, they might manage a GitHub enterprise account available for all stakeholders in the organization. Alternatively, this is solely an engineering function, though the OSPO may set the procedures and vetting rules for inbound software.

Integration with Threat Intel, Security and Incident Response

It's a best practice to integrate SBOMs with relevant areas of security operations, including threat intelligence, which picks up on known threats. The team handling threat intel should be able to reference SBOMs in near real time to determine if any of the organization's software is at risk.

If the threat intel team matches a threat to a component of the SBOM, then they need to issue an alert or trigger an incident response workflow. This workflow should also integrate with the SBOM, so developers and related security stakeholders tasked with remediating the problem will be aware of the circumstances—and allow for the SBOM to be updated once the malicious component has been replaced.

How Revenera Handles SBOMs

As an OpenChain (ISO/IEC 5230:2020) conformant software company, Revenera follows its own guidance and approaches SBOMs using best practices. Our comprehensive OSS management program covers roles and responsibilities, policies, generation of compliance artifacts (including SBOMs), incident response procedures, training requirements, and stakeholder accountability. At a foundational level, our SBOMs are based on the concept of accountability. Those who are responsible for using code components in software are accountable for any security or software compliance license risks that arise through their use. Roles and responsibilities define who is therefore responsible for updating SBOMs creating any compliance artifacts required by use of the components in question. Employees are provided foundational training on both opens source licensing and security topics. Additional training is provided on our internal policies and procedures.

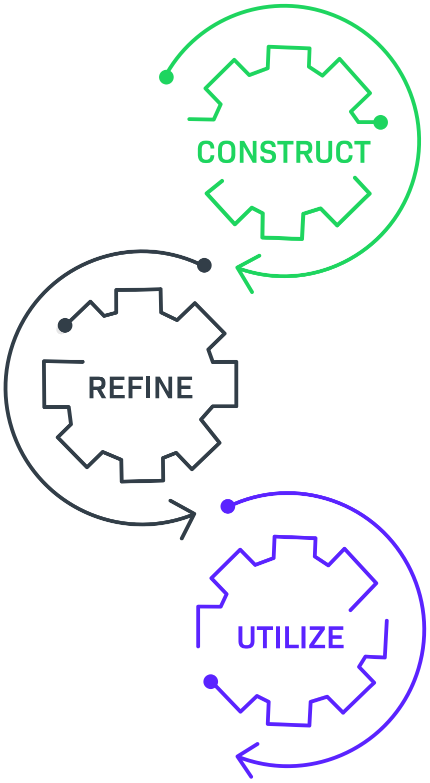
The Revenera SBOM program is based on two key elements of our OSS policy. Everyone must understand and comply with OSS license obligations, and the product team reviews all associated security vulnerabilities for both relevance and impact to their respective products. The OSPO and security teams assist as-needed with all OSS management activities. For compliance issues, we create remediation tasks in JIRA, which are then worked into the product backlog by the product owners.

As part of our Cybersecurity Checklist, we use Revenera Code Insight to do continuous scanning. We perform SCA scans of our proprietary codebases and build artifacts to catalog all third-party dependencies in SBOMs. We monitor existing SBOMs for new and updated vulnerabilities and pay attention to old component versions even if there are no reported vulnerabilities. Our goal is to be able to assess and remediate legal and compliance issues on a continuous basis. We also produce compliance artifacts, including third-party notices, SBOMs in multiple formats (CycloneDX, SPDX, and human-readable HTML & Excel), and third-party source distributions when required by the OSS license.

Revenera for SCA and SBOM Management

Revenera provides a comprehensive set of solutions to help organizations manage all of their SBOMs—those created internally and any coming from external sources. Both Code Insight and SBOM Insights from Revenera cover the complete lifecycle stages of an SBOM:

REVENERA FOR SCA AND SBOM MANAGEMENT



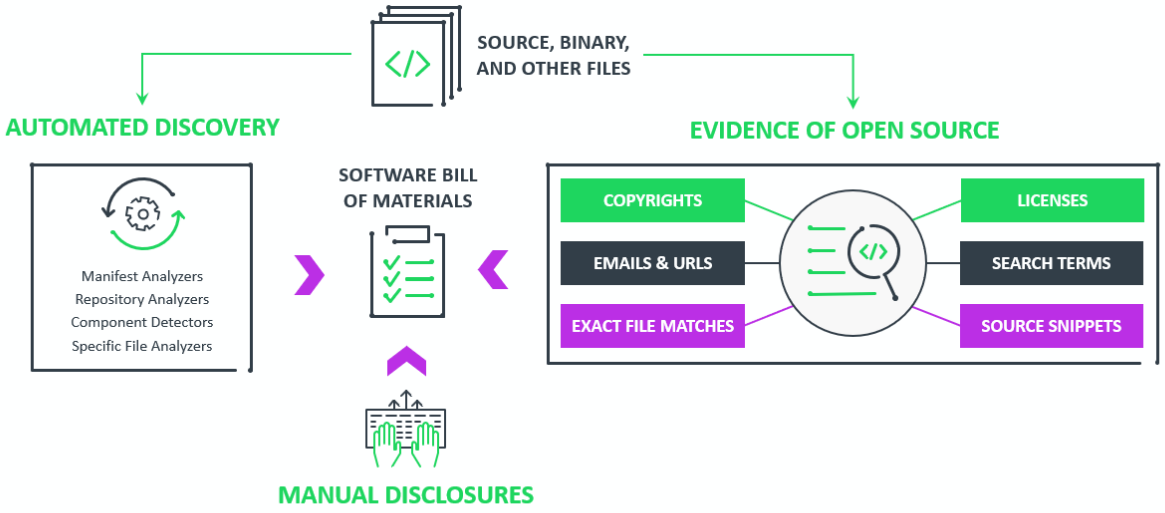
CONSTRUCT
Your SBOMs representing your portfolio of applications consist of parts that come from many different places, both inside and out of your organization. This phase takes all that SBOM data—including open source components, third-party code, and commercial—reconciles it, and presents it in an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

Revenera's Code Insight helps reduce open-source security risk and manage license compliance with an end-to-end system. It is a single solution for open-source security and license compliance that integrates into development and IT environments. Code Insight is an SCA tool and code scanning platform that also performs vulnerability monitoring and SBOM creation tool. The Code Insight solution delivers a complete, accurate SBOM for all applications, enabling users to analyze risk quickly with detailed dashboards and reporting. It supports dozens of programming languages for deep scan and analysis of source code fragments to assess copy/paste scenarios with OSS or third-party code. Code Insights gives users vulnerability data from multiple data sources including the National Vulnerability Database (NVD), RubySec, RustSec, Debian security advisories, and our own primary security research team, Secunia Research. With Code Insight, organizations can define and enforce policies for security and license compliance

END-TO-END SCA SOLUTION FOR LICENSE COMPLIANCE AND SECURITY RISK MANAGEMENT



revenera
SBOM Insights®

SBOM Insights from Revenera iis a cloud-based SBOM management solution that collects information from anywhere in an 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. Users manage security and legal risk by maintaining an actionable SBOM for more supply chain control and transparency. With all open source code and third-party components catalogued, when the next high-profile vulnerability hits, developers and security teams have access to unified data to quickly uncover potential exposure and fix problems—both in the code internally scanned and in the software components coming from outside the organization.

SBOM SOURCE OF TRUTH

COMPLIANCE ARTIFACTS

IMPACT ANALYSIS

USAGE INSIGHTS

ALERTS

Conclusion

Open-source components and packages are a boon to software development, enabling developers to move more quickly and take advantage of proven code. At the same time, use of OSS creates security risks and exposes software producing organizations to potential issues with licensing compliance. Producing and maintaining an accurate, complete SBOM is an answer to ongoing maintenance and software supply chain management.

The SBOM is an organized mechanism that helps organizations understand the composition of its software. It supports security policies that protect software against supply chain attacks, e.g., being able to react quickly and accurately to a threat like Log4j. When application contents are well catalogued, it is possible to assess impact of a supply chain attack by doing a simple vulnerability search. The SBOM also facilitates compliance with relevant licenses and prevents passing potential risk to downstream users.

A well-prepared SBOM benefits the business. It can contribute to more efficient development, security and IT operations while improving relationships with customers, partners and the open-source community. To achieve these benefits, the SBOM has to evolve beyond the traditional manually prepared list of software components.

SBOMs are produced using automated, intelligent tools like Revenera's Code Insight, which offer greater completeness and more up-to-date information about what's in a software application. When produced in alignment with emerging best practices, such SBOMs make it possible to derive maximum value from open-source code while mitigating the associated security and licensing risks.

Build Better Products

With Software Composition Analysis (SCA) from Revenera you can build better products and quantify what matters. Our solutions help you discover, assess, and manage license and security risk across all your software applications. Our mission is to support the construction of a complete and accurate SBOM to manage Legal and Security risk, and deliver compliance artifacts required by your compliance programs.

With SCA from Revenera you can manage a complete SBOM in a SaaS environment. Ingest SBOM data from a wide range of sources and unify internal and external SBOMs across your organization into a single actionable view. Additionally, discover and track all open source, third-party, and commercial software while managing open-source license compliance, reducing IP risk, and identifying and fixing vulnerabilities.

NEXT STEPS

Learn how Revenera can help you protect your applications, manage compliance, understand customer needs and drive recurring revenue.

LEARN MORE >

Revenera 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.revenera.com**

revenera
1.800.809.5659 | +44.870.871.1111 | revenera.com