WHITE PAPER

revenera

Risky OSS: How Regulated Industries Can Secure the Software Supply Chain

4 Open Source Management Use Cases Lead The Way

What's Inside

The software supply chain is the backbone of organizational innovation and growth— but it's also a source of significant risk. A growing reliance on Open Source Software (OSS) and third-party components drives up complexity, making effective management efforts more important than ever. This whitepaper reviews the state of OSS, four management use cases, and best practices and solutions that help security and legal teams in highly regulated industries like energy, finance, medical devices, transportation/ automotive, and publicly traded companies confidently mitigate rising supply chain risk.

The Value of Open Source Software

OSS now comprises 80 percent of all proprietary applications.

Modern-day Open Source Software (OSS) is extremely popular for creating derivative works. Its preexisting, proven components spur innovation, speed up time to market, come with broad community support and expertise, and it's free to use. For these and other reasons, developers are now integrating it into more than 80 percent of proprietary applications. But with this freedom comes obligations and responsibilities.

INSIGHT

86% of developers say they sometimes or always try to find open source options over other kinds of software

Savvy organizations, particularly those in highly regulated industries, recognize the criticality of mitigating security vulnerabilities associated with OSS and the legal risk of failing to comply with applicable licenses that outline explicit terms and conditions for use.

Relying on OSS should be a strategic decision to improve product quality and gain a competitive edge rather than a quick, cost-saving measure.

Before using OSS packages in commercial software, it's essential to understand open source trends and associated risks.

Key OSS Influencers

The software supply chain's perfect storm.
Four primary trends are shaping the open source software industry today.

1. Growing OSS code popularity. More than thirty years after the idea of open source software was first proposed, companies today rely extensively on OSS for mainstream usage and to support proprietary software builds. It enables developers to work at an accelerated pace and drives innovation. Without it, companies are slower to market and provide customers with less value than competitors who use it.

Revenera Audit Services discovered more than 2,929 OSS components in client applications in 2024. Ten years ago, that number was in the low hundreds. BCG Research found that 80 percent of IT departments have plans to increase OSS use. OSS is used everywhere, and reliance continues to grow year over year.

2. Rising security exploits. As the use of OSS increases, so does the importance of securing it. The software supply chain is constantly threatened by a growing number of increasingly sophisticated exploits. Global criminal organizations, nation-states, and other threat actors invest significant time and resources to hack commercial applications and products for financial gain. Nothing is off-limits. Attacks can target any area across the software including OSS components. Successful breaches always have far-reaching, costly implications.

Identifying vulnerabilities is no trivial task, especially when a single application consists of multiple components and code sources. Adding further complexity, many different security databases (public, commercial, and vendor-specific) continuously publish vulnerabilities as they become known, with varying levels of severity according to the Common Vulnerability Scoring System (CVSS).

3. More regulations. Security failures pose serious risks — so does a breakdown in license obligations. For these reasons, more regulations have been passed to ensure transparency across the software chain so that vulnerabilities are quickly mitigated, license requirements are met, and software can be more secure for the companies that build it and the users who rely on it.

A growing number of regulations require more transparency with a Software Bill of Materials (SBOM). The U.S. Cyber Security Executive Order (2021) from the Biden Administration mandates SBOMs for any software sold to a federal agency. European companies must adhere to the Cyber Resilience Act, and industry-specific regulations exist for finance, medical devices, transportation, energy, and publicly traded companies.

4. Disconnected supply chain. The regulatory requirements that call for more visibility seek to elevate the otherwise complex, disconnected process of producing software. Applying this goal to a hardware example makes it easier to understand.

When manufacturing a car, it's easy to unwind the supply chain and see which supplier contributed a part, like the engine or the transmission. This is much more difficult in software because the supply chain is disconnected. The provenanceof parts, understanding who supplied what, the precise code used, vulnerabilities it may have, and how it gets fixed when an issue arises isn't as clear-cut as the implications of an engine failure in the car manufacturing example. OSS users are ultimately responsible for all of the code they produce. A lack of transparency too often leads to a lack of accountability.

OSS Can Be Risky Business

Most security and development teams are aware of less than 10 percent of the open-source software used in their applications.

217%
YOY increase in codebase security vulnerabilities

27%
of security vulnerabilities have a high CVSS severity rating

7%
YOY increase in binaries

To manage software supply chain risk, quick identification and remediation of security and legal risk is essential for all organizations, but especially for highly regulated industries that include finance, medical devices, transportation/automotive, energy, and publicly traded companies.

Manage Security and Legal Risk with SBOMs

Build an accurate inventory and discover actionable risk mitigation insights for your organization and customers.

One way organizations gain greater visibility of their OSS and mitigate associated risks is with a Software Bill of Materials (SBOM). A precise inventory of the components in their code, an SBOM can deliver critical, timely intelligence for software producers and users.

SBOMs ensure a more secure software supply chain. They will:

- **Identify open source, third-party, and commercial components used in your software supply chain and associated security vulnerabilities**
- **Pinpoint potential license compliance issues**
- **Identify security vulnerabilities and support swift response**
- **Eliminate time-intensive, manual efforts that take developers away from more strategic projects**
- **Keep customers up to date on the software they rely on**

If you work in a regulated industry like finance, medical devices, transportation/automotive, energy, a publicly traded company or your organization sells to government agencies, an SBOM is table-stakes.

What Does an SBOM Include?

An SBOM is complete, machine-readable code documentation. The queryable record includes details from multiple sources about a software application's connected components, versions, and dependencies. It accounts for all the commercial libraries, proprietary software, open-source dependencies, and information on the suppliers and code authors. Ideally, licensing information and security vulnerability reports are also included.

Think of an SBOM as a list of ingredients on food packaging. With a complete list of components, companies can better understand the software supply chain and manage organizational risk accordingly.

INSIGHT

Selling software to a U.S. government agency? SBOMs are required.

The U.S. Cybersecurity & Infrastructure Security Agency (CISA) defines a Software Bill of Materials (SBOM) as a formal record containing the details and supply chain relationships of various components used in building software. These components, including libraries and modules, can be open source or proprietary, free or paid, and the data can be widely available or access-restricted.

The Executive Order (EO) from the Biden administration requires any company that sells software to a federal government agency to provide SBOMs. The hope is that this public-sector requirement will encourage other industries to follow suit.

Create a SBOM with Software Composition Analysis (SCA) Tools

Growing application portfolios and an increasing reliance on OSS often result in large, complex SBOMs. Software Composition Analysis (SCA) tools ingest and unify large volumes of internal and external data to publish accurate, complete SBOMs for actionable insights that mitigate security vulnerabilities and operational risks.

60% of organizations building or procuring critical infrastructure software will mandate an SBOM by the year 2025

86% of developers said they sometimes or always try to find open source options over other kinds of software

81% of organizations are moderately to highly concerned about risks surrounding suppliers and partners.

Gartner Defines SCA

Gartner defines SCA as a technology that analyzes applications and related artifacts (containers, registries, etc.) to detect open source and third-party software components known to have security vulnerabilities, are out-of-date for security patches, or that pose licensing risks. SCA products and services help ensure the enterprise software supply chain includes only secure components and, therefore, supports secure application development and assembly.

INSIGHT

Revenera delivers end-to-end SCA solutions for complete, accurate SBOMs while managing license compliance and security.

READ OUR CUSTOMER REVIEWS AT GARTNER PEER INSIGHTS >

4 SCA Use Cases for OSS Management

Proactively managing your OSS with SCA tools will improve the security of your supply chain, here are 4 common use cases.

1. Inbound assessments

Anytime something new is brought into an organization, there is risk. Before a developer pulls in a large library, an upstream partner or contract developer integrates code into the company code base, or new code is brought in during an M&A or divestiture, an inbound assessment will weigh risk and reward. In these examples and others, an inbound assessment can help identify vulnerabilities and determine if they align with company policies before anything is added.

2. Perform internal compliance checks

The earlier you discover an issue, the easier and less costly it is to address. The more time that passes after code has been developed — perhaps the developer left, forgot about it, or there's been a change in team composition — the more difficult problems are to identify. Internal compliance checks are an important part of a software development lifecycle's overarching Shift-Left Strategy and can be integrated into the dev environment with continuous information flow.

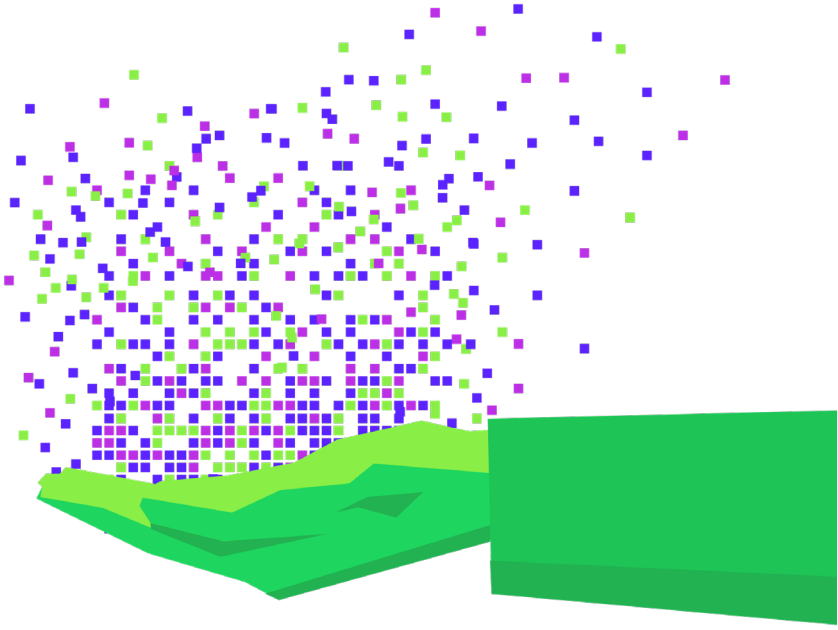
3. Meet industry and customer demand

Few things move a company to action faster than industry and customer demand. A growing number of companies are being asked to provide SBOMs with every software sale. A wide range of industry regulations are now in place, and if you sell to any publicly traded company, they will also need an SBOM. Software transparency with accompanying security reports and attribution fulfillment are important ingredients to successful partnerships and this use case is quickly becoming a leading forcing function for the use of SCA tools.

4. Respond to an event

Unfortunately, some organizations wait for something to go wrong before they look at their software supply chain. Without a complete outline of all components used and the dependency tree, a newly published security vulnerability or regulatory compliance concern becomes an emergency search, and teams are on their heels trying to catch up. More importantly, when an industry wide security vulnerability shows up, teams scramble to find which products are impacted.

How Revenera SCA Solutions Help



Best practices for managing your OSS.
Here's a look at how SCA solutions from Revenera can address each of the four mentioned use cases.

Dependency assessments

Dependency assessment tools can be used by developers who have written code and want to ensure all application dependencies are represented on the dependency tree. They identify the security vulnerabilities and licensing issues associated with the application dependencies before it is committed to the code base. Organizations use them to ensure all incoming dependencies are compliant with company policies and the licenses are allowed and confirm that security vulnerabilities that come with direct and transitive dependencies are visualized, assessed, understood, and agreed upon.

These assessments can be done within a dev environment or integrated into the DevOps process as part of build pipelines. The goal is to gain insights and make necessary changes before introducing any code —they proactively address risk and improve software engineering efficiency.

The Revenera OSS Inspector IDE Plug-in enables developers using IntelliJ IDEA (an Integrated Development Environment, or IDE) to examine—within the IDE itself—the licenses and security vulnerabilities associated with the OSS components used in their application code before introducing any new components into the company code, saving time and avoiding costly issues later. Security vulnerabilities can be assessed within the IDE, and it will prevent the injection of components with copyleft licenses from the outset, ensuring that your code remains compliant from the start.

Third-party notices

While open source software is free, it comes with its own obligations. An early indication of compliance issues minimizes disruptions for the engineering team and improves team efficiency. As part of a Shift-Left strategy, SCA tools can be integrated into either the IDE or the design/build process to prepare third-party notices to satisfy the OSS license attribution requirements. It allows the identification and remediation of security vulnerabilities early in the process before they become much more problematic and expensive to resolve.

To help companies remain compliant and provide legally required attribution, Revenera Code Insight automatically satisfies this requirement by generating complete SBOMs in multiple formats (CycloneDX, SPDX, and human-readable HTML and Excel) and Third Party Notices reports. The complete, up-to-date library of actual license texts associated with open-source component versions eliminates time-consuming, manual efforts to identify and collect license texts for OSS components.

Security reviews

While company code won't change unless intentionally modified, new security vulnerabilities emerge regularly, and some are more critical than others. Easy analysis and prioritization are essential to effectively lower risk, maximize the time and effort of security teams, and, for highly regulated industries, ensure compliance.

Revenera Code Insight identifies vulnerabilities throughout the software development lifecycle—from development to production. Discover security vulnerabilities by scanning the software and prioritizing remediation with a view of the vulnerability description, security source, severity, and remediation steps, including patch links. With this level of detail, security teams can assign risk based on how the application is deployed and used.

SBOM management

SCA tools can support the entire SBOM lifecycle, including constructing an SBOM, reconciling, refining, and remediating SBOM parts, and fulfilling outbound SBOM obligations.

Revenera SBOM Insights can collect and ingest SBOM parts from multiple sources to create an SBOM in a SaaS environment, aggregate that data into a single repository, and provide full visibility for security, legal, and downstream supply chain partners to act on the results. The solution also provides ongoing risk reports for license compliance and security risks.

Impact analysis

Situations will arise where an immediate look into your applications and all their components is necessary. Your customer reports a vulnerability; there is a report of a new hack in the news. Maybe an audit demands proof of license compliance. In each instance, an investigation must be conducted quickly to understand how the software supply chain and its users are impacted.

SCA tools from Revenera can quickly generate a global inventory view that includes all OSS, third-party, and commercial components, vulnerabilities, impacted components, and license status. This easy report generation is the pay-off for implementing a comprehensive approach to SCA. Instead of a painstaking, time-consuming search for what's happening in your software environment, you can deliver a faster, more accurate response.

Get Started in 3 Steps

Proactively managing OSS is the key to improving the security of your software supply chain. Follow these three steps to get started today.

1. Operate within a security framework. Adopt a security framework to follow best practices across your software supply chain. The National Institute of Standards and Technology (NIST) is a cybersecurity framework that helps organizations promptly identify, manage, and counter cybersecurity events. Together with your organization's Chief Information Security Officer (CISO), work to align organizational policies and processes with the framework and your industry specific regulations to safeguard data and mitigate risk.

2. Develop and maintain an OSS policy. Including code from anywhere without validation isn't an option—the risks are too high. Instead, define your organization's OSS license and adoption policies, update them regularly, and maintain alignment with industry regulations.

3. Generate SBOMs. If your customers haven't asked for SBOMs yet, they will soon. Start creating complete, accurate SBOMs for your applications. SCA tools will help your organization gain transparency and generate accurate, timely SBOMs that track all the components in your software.

NEXT STEPS

Gain transparency and actionable insights into the complexity of your software and meet industry regulations with Revenera.

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