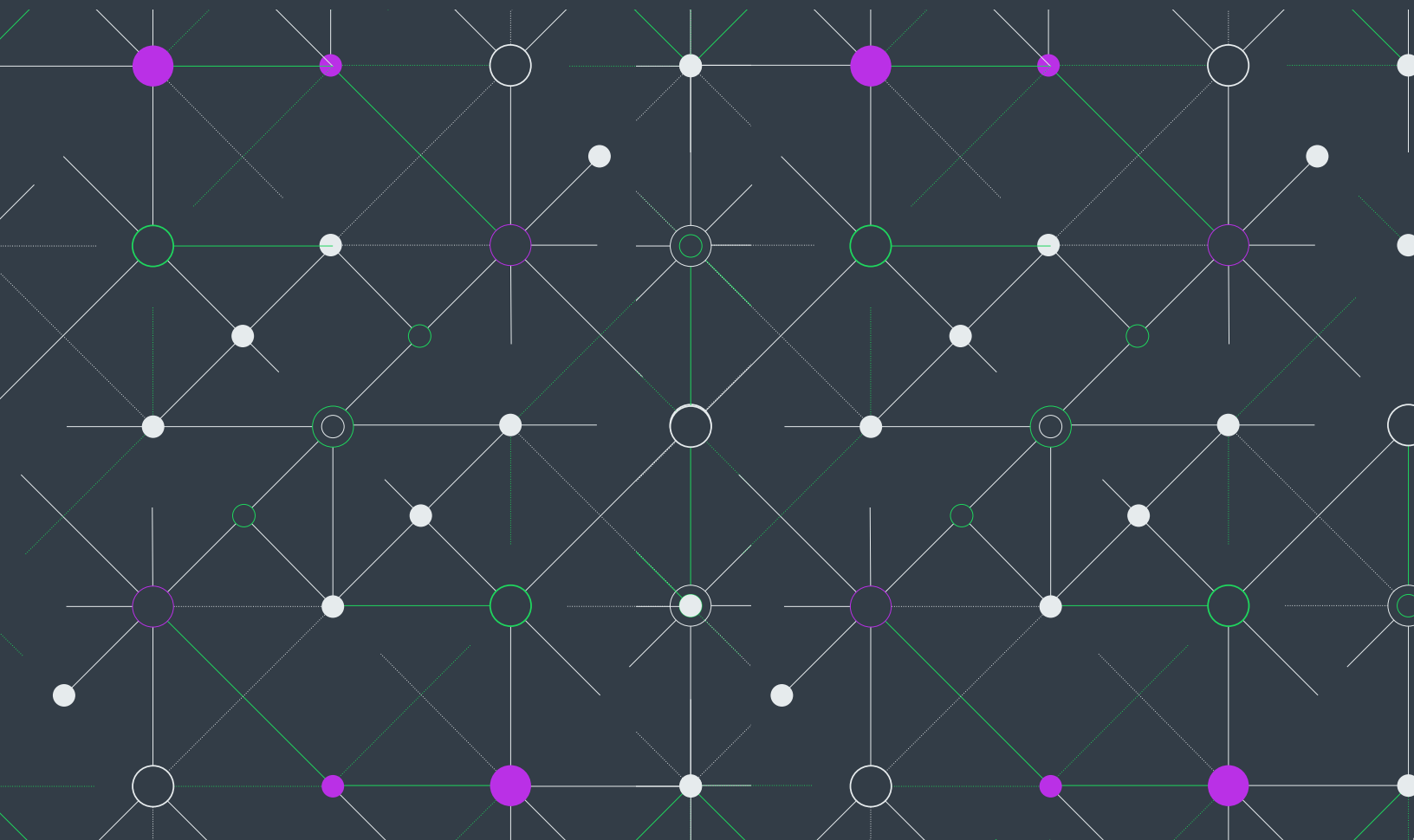
INDUSTRY REPORT

revenera

The 2022 State of the Software Supply Chain Report

Key Insights



Introduction

This report compiles the data from over 100 Revenera audit services projects in order to identify the latest trends related to what companies know about the open source software (OSS) in their applications, the associated license compliance and security risk, and severity of discovered issues. As the use of open source continues to go up, as well as increased attacks on the software supply chain, this report is critical to understanding how to better seize the opportunities provided by OSS while protecting IP and potential revenue loss from increased risk.

Executive Summary

In our 2021 report, with the upheaval caused by COVID-19, we stated that the prior year "represented the stampeding herd over the hill." Things didn't get much better. In fact, COVID stuck around and fundamentally changed the way we both live and work, and how companies engage with, sell to, and keep customers. As a result, the digital supply chain has never been more important—and it's under attack. 64% of organizations have been impacted by a software supply chain attack in the last year[1]. To make matters more alarming, most teams lack the resources, budget, and knowledge to manage a crisis.

The software industry's reliance on open source, along with a sharp increase in OSS dependencies and the frequency of newly reported security exploits has set up a perfect storm for supply chain security[2]. In the past, companies prided themselves in developing 100 percent of their own code. Today it would be difficult to find a company that does not leverage a multitude of OSS components in order to accelerate time to market and make use of community-developed and tested capabilities. Code may be farmed out to a partner, a vendor, contractor, or various other companies that build on top of each other's code to create a final application. There's code in-house developers write and there's supplier code. All of these are entry points into the software supply chain. It's imperative for companies to have a deep understanding of the supply chain to be able to control potential unknown risk.

64%

of organizations have been impacted by a software supply chain attack in the last year

[1]Anchore, Anchore 2021: Software Supply Chain Security Report

[2]Alex Rybak, Incorporating SCA Into Your Application Security Strategy, May 2021

The industry and markets continue to respond to software supply chain and security risk by increasing regulations aimed at discovering and tracking open source issues. NIST, PCI, OpenChain, OWASP, MITRE, NHTSA, and GDPR are just a few of the organizations that put in place new or additional guidelines meant to minimize security and compliance risk. In May the U.S. Government initiated a Cybersecurity Executive Order (EO) that includes new security requirements for software vendors selling software to the U.S. government. The EO puts the Software Bill of Materials (SBOM) center stage now and into the future by stating that any software provider that sells software into the federal government must provide an SBOM. The private sector is following suit. This year at least a third of organizations are planning on complying with the Executive Order[3] while 43 percent believe they need assistance with all the emerging regulatory and compliance requirements[4].

2021 further illustrated the greater need for companies to consider their tech stacks. The use of open source creates a requirement for organizations to implement a Software Composition Analysis (SCA) solution to empower development teams to leverage the benefits of third-party software in the devops lifecycle while minimizing OSS security and license compliance risk for customers, partners, and end users.

To help companies better understand the current state of license compliance and the role compliance plays in enhancing transparency and control while minimizing risk, Revenera developed the ***2022 State of the Software Supply Chain*** report[5]. This report helps security, software development, and legal experts understand market trends and benchmark their own efforts against others.

What is Software Composition Analysis?

Software Composition Analysis includes products and services designed to support:

- Cataloging the usage of open source and third-party software
- Managing intellectual property and security risks
- Operationalizing organizations' open source strategy
- Detection of OSS components regardless of how deep those components are embedded in the codebase
- Delivering a complete and accurate Software Bill of Materials (SBOM) to customers and downstream supply chain partners
- Increased transparency into the software supply chain

[3]Anchore Security, 2022 Anchore Security Report

[4] Forrester Opportunity Snapshot: a custom study commissioned by Perforce, April 2021

[5] The analysis includes findings from the anonymized data of 105 audit projects in 2021

Revenera analyzed audit projects from 2021 to look at the difference between open source awareness and actual open source use. The numbers show that, still, most companies are not aware of most of the open source components they are using and, as a result, face license compliance issues and unknown potential exposures to security vulnerabilities in their applications.

Revenera also performed analysis on the types of audits being performed as well as the priority level of uncovered issues. Companies looking to perform audits of their open source use can better understand when a deep dive is needed, the extent to which they are vulnerable to high priority, high-impact problems, and the critical path to issue remediation.

General Analysis Numbers

- Cross-industry
- Global[6]
- 230,964 total issues uncovered
- Over 2.6 billion lines of code

Open Source Use Awareness

Awareness of the potential security and license compliance risk your organization faces is the first step to building and maintaining a successful open source management strategy. However, close to 70 percent of organizations do not have company-wide policies for properly using open source, identifying associated security vulnerabilities, and complying with the requirements of the associated open source license[7].

The Revenera audit team identified 12 percent more issues in 2021 (over prior year) with 2,200 issues uncovered per audit project compared to 1,959 in 2020. 61 percent of the scanned codebase files were attributed to open source, up 6 percentage points from 2020. However, only 17 percent (13,068) of the 230,964 issues eventually uncovered during the audit process were disclosed prior to audit start. Disclosure is trending in the right direction, up over 10 percent from 2020, but the gap is still considerable.

▲ 12%
in discovered issues compared to 2020

61%
of the scanned codebase files were attributed to open source components;
▲ 6% from 2020

17%
of the issues uncovered were disclosed prior to audit start
▲ 3% from 2019

2,200
was the average number of issues uncovered per audit projects;
▲ 12% in issues compared to 2020

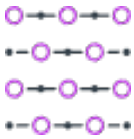
[6] Majority of audits coming from the U.S. and EMEA
[7] Forrester Opportunity Snapshot: a custom study commissioned by Perforce, April 2021

SCA: More Important Now Than Ever

Open source is more pervasive now than ever. Organizations increasingly turn to OSS to power digital transformation and drive efficiencies and flexibility into their applications. Without a comprehensive strategy to govern the use of open source, organizations risk missing out on the benefits it can deliver.

The number of binaries in a typical application codebase continues to go up. Compared to source code, binaries are more complex in that they often have combined IP from multiple sources and are made up of many constituent files. Revenera found a 7 percent increase in binaries compared to 2020. With both the maturity and complexity of the software supply chain, it's more important than ever to better understand what's in your code. Additionally, Revenera discovered 11,500 lines of code for every uncovered issue—a 5% increase compared to 2020.

> ***"Understanding your organization's risk from open source software, in terms of both "how likely" and "how much impact," is the key to making well-informed business decisions...which can start by investing in a Software Composition Analysis of your own codebase."***
>
> *- Derek Brink,*
> *"Open Source Software: To Get More Value, Manage Your Risks"*



343,000
binaries
↑ 7% YOY

11,500
codebase files for every 1 identified issue

License Compliance

The issues uncovered in codebase scans related to license compliance vary in severity and remediation approaches.

Revenera assigns priority levels to issue detection, with Priority 1 (P1) issues being the most critical to remediate first and quickly because they pose the most critical threat. The Revenera audit team found over 9,500 P1 issues. One out of every 25 license compliance issues uncovered by an audit were considered P1s which represent items with significant business impact and typically requiring a sense of urgency and fast remediation.

Revenera Issue Detection Priority Level Definition

Priority Level	Description	Revenera Recommendation
P1	High severity issues such as strong Copyleft compliance issues involving the APGL and GPL, or other important vulnerabilities.	Remediate and fix P1 issues first and with urgency because they represent a critical IP security threat.
P2	Secondary priority issues related to commercial and vanity licenses.	Create a plan to resolve these issues after P1 threats are remediated.
P3	Low risk hygiene issues related to permissive license issues such as those under BSD, Apache, and MIT.	Not to be ignored long-term, but certainly a slower, more systematic remediation approach is acceptable.

Identified Issues by Priority Level

		vs 2020
P1	**4%**	▲ **6%**
P2	**3%**	▲ **50%**
P3	**92%**	▲ **34%**
other	**1%**	▲ **7%**

Deep Code Scanning versus High-Level

The Revenera audit services team conducts several types of audits, based on client request, timing, scanning depth, and need:

- **Forensic Audit Analysis** – Performs an in-depth, deep level scan of all evidence types.
- **Standard Audit Analysis** – Identifies explicit P1 licenses and large third-party components.
- **Targeted Audit Analysis** – Custom audits based on customer need; usually targets specific areas of the codebase.
- **Other** – Hybrid of any of the above audit services types.

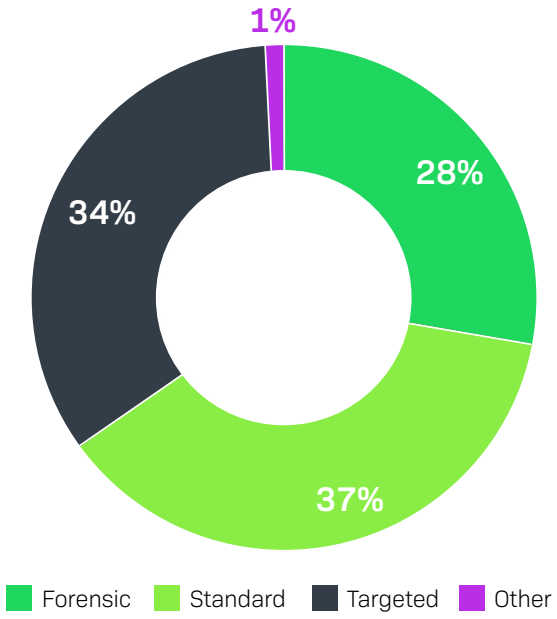
Compared to 2020, the audit services team conducted about 15 percent more Forensic Audits. The number of Standard Audits went up by 3 percent, and targeted audits represented 12 percent of all audits conducted in 2021, down from 2020 by 35 percent. Audit customers expected faster turnaround times in 2021 due to an increase in M&A activity. According to a KPMG report, global deal makers announced $5.1 trillion worth of M&A transactions in 2021; up from $3.8 trillion in 2020[8]. 80 percent of executives expect that number to grow higher in 2022.

Similarly, Revenera conducts audits for specific events like M&A activity, providing a complete risk profile and forensic report along with a remediation assessment for clients. The team found 103 P1 issues per project representing 5 percent of the total issues uncovered. 65 Priority Level 2 (P2) issues per project were discovered.

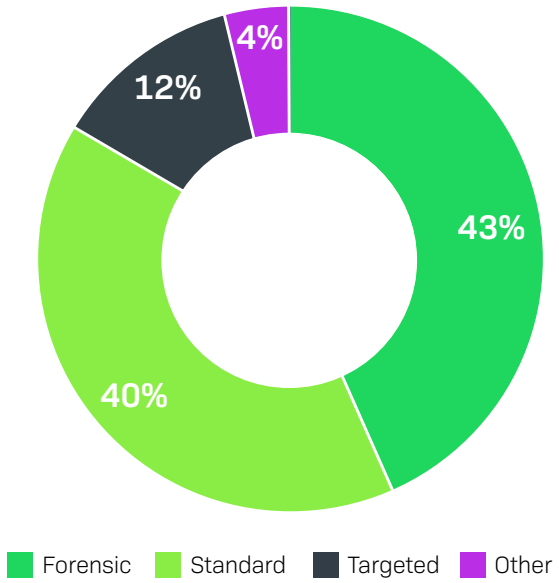
Issues Discovered in M&A and Baseline Audit Projects

Priority Level	M&A Audits: Issues/Project	Basline Audits Issues/Project
P1	103	40
P2	65	24
P3	2,280	989
Other	18	10

Issues Discovered by Audit Type - 2020



Issues Discovered by Audit Type - 2021

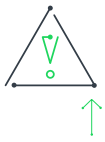


[8] KPMG, 2021 Was a Blowout Year for Global M&A, January 2022

Security Vulnerabilities

Software supply chain attacks grew by more than 300% in 2021 compared to 2020, according to a study by Argon Security[9]. Attackers are focusing more heavily on open source vulnerabilities and exploiting the software supply chain and supplier trust. Despite that, the level of security across the software development lifecycle remains low.

Revenera's audit team uncovered 282 security vulnerabilities per audit project, an increase of 217 percent over 2020[10]. 27 percent of those vulnerabilities have a "high" CVSS severity rating.



217
security vulnerabilities per audit project;
217% from 2020

27%
are security vulnerabilities with a "high" CVSS rating

Major Cybersecurity Attacks in 2021

2021 brought more sophisticated cybersecurity adversaries, more pervasive threats and more damage, quicker, thus the need for increased regulatory compliance. Here are some of the more high-profile, significant attacks from last year:

December '20/January: SolarWinds - Russian attackers compromised about 100 private corporations in the United States and nine federal agencies' networks.

January: Microsoft Exchange - Chinese hacking group Hafnium found vulnerabilities in Microsoft Exchange that gave them access to the email accounts of at least 30,000 organizations in the U.S. and 250,000 globally.

May: Colonial Pipeline – The criminal group DarkSide breached Colonial Pipeline's systems and shut down a major fuel supply for the East Coast. Colonial Pipeline's CEO ultimately authorized a $4.4 million ransom payment to restore the systems. This particular attack showed that US infrastructure was not immune from malicious software attacks.

December: Log4j - A zero-day vulnerability in the popular Apache Log4j open source logging library used in nearly every enterprise app and service from vendors including Microsoft, Twitter, VMware, Amazon, and Apple, among others. Shortly after Apache disclosed the remote code execution vulnerability (CVE-2021-44228) on Dec. 9 and released a patch, threat researchers and the U.S. Cybersecurity and Infrastructure Security Agency sounded the alarm that attackers were already exploiting the security flaw, which received a perfect 10 out of 10 CVSS score. Over 1M hacks have exploited the zero day vulnerability, and the impact to these exploits is not yet fully known.

[9] Argon Security, 2021 Study

[10] Data is based on Forensic and Standard audits.

Open Source Licenses

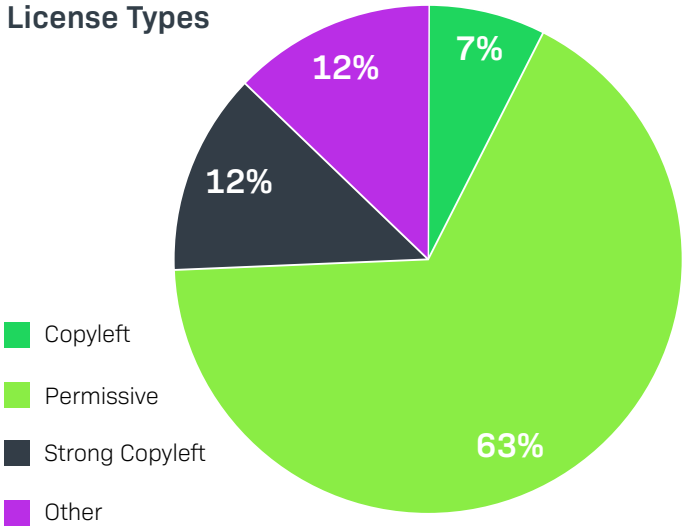
Gartner estimates fewer than 50 percent of organizations have adopted SCA tools, although they predict adoption will increase steadily given the imposed operational risks and the increased need for transparency and an SBOM[11]. This is made more imperative given 39 percent of companies are not confident that their open source components are up to date, secure, or well maintained[12]. SCA tools focus on identifying and providing warnings regarding licenses that may impose terms that are unacceptable to an organization. Ideal solutions offer reports on both direct dependencies (those explicitly invoked by the developer) and transitive dependencies which account for a very long tail of OSS components pulled into an application by the libraries that the application depends on to work.

Open source licenses present a wide disparity in the rights they grant and the imposed obligations. A number of widely used open source packages have no one maintaining them, which increases the overall risk of exploitation since no one is at the wheel releasing patches for security fixes. It is critical for security, compliance, development, and legal teams to know which ones are in dependencies to better understand the potential impact on the software supply chain.

- Across audit services projects in 2022, weak copyleft licenses made up almost 7 percent of the scanned codebase, meaning the software program is free and all modified and extended versions of the program should also be free and released under the same terms and conditions. Developers have the right to use, modify, and share the work as long as the reciprocity obligation is maintained.
- Permissive licenses made up 63 percent of the codebase. Permissive licenses have minimal restrictions, ensuring the freedom to use, modify, and redistribute, while also allowing proprietary derivative works. Typically, all that is required is giving credit to the author via proper attributions.
- Strong copyleft licenses comprised 12 percent of the audited codebases. These licenses mandates that any distributed software that links or otherwise incorporates such code be licensed under compatible licenses. The entire work is impacted by the license and not just modified code as is the case with weak copyleft. These licenses have also been called “viral”.

[11] Gartner, Market Guide for Software Composition Analysis, September 2021
[12] The Tidelift Guide to Managing Open Source, Tidelift, January 2022

Developers and engineering teams know that open source licenses are important and that they matter. License confusion or not understanding the demands of the thousands of licenses that exist can ultimately have enormous business impact if issues lead to possible litigation. It is crucial that every company identifies its own risk tolerance for license use and create policies around what is acceptable.



The SBOM: Just the Beginning

2021 was the year of the SBOM as the key artifact for an open source governance process. Driven in large part by a broadening array of stakeholders who need access to its contents and regulatory requirements such as the U.S. government's Cybersecurity Executive Order, the siloed approach to building an SBOM and static way of viewing the data is evolving into an automated, collaborative, and dynamic process.

The sheer number of dependencies and increasing ecosystem (there were 61 million new repositories created in 2021 on GitHub alone[13]) broadens the plane for risk. You simply can't comply with and secure what you don't know is there.

There's now a business mandate for increased visibility into the software supply chain that eclipses legal and security teams and now includes, for instance, those responsible for quality assurance, product safety and export compliance.

As industries and governing bodies increase governance requirements and more companies require an SBOM from software suppliers as part of the contractual process to prove software supply chain security, having a complete, accurate inventory of what's in code will most likely become the norm rather than the exception.

> ***"Producing a comprehensive Bill of Materials is perhaps one of the most important actions for development teams. You can use it to modify open source policies and quickly react to published vulnerabilities. A BOM lets you know exactly what's in your code."***
>
> *- Wind River Systems*

[13] The 2021 State of the Octoverse, Vol. VI,

Bottom Line: Secure the Software Supply Chain

The software supply chain is under attack and all indications say bad actors are going to step up their exploits in the coming year. The use of open source software will continue to increase, creating a greater need for Software Composition Analysis solutions now more than ever.

Supply chain attacks are increasing exponentially.

Here are six steps to take now to better secure the software supply chain:

1. Understand the construction of the software pipeline and how software sources, components and packages gain entry.
2. Produce a precise SBOM that includes all subcomponents, hidden dependencies and associated licenses.
3. Shift vulnerability management and license compliance left to minimize and mitigate open source risk early in the devops lifecycle. Early detection of issues is key to releasing applications on time to customers that is risk-free.
4. Collaborate with key stakeholders across the organization including Security, Software Development, Legal, and Executives to create documented policies regarding open source use. Consider creating an Open Source Review Board tasked with the development, communication, and operationalization of an open source strategy.
5. 30% of organizations say having access to open source training will enable successful OS strategies at their organizations . Empower software developers by providing ongoing education for security vulnerability and license compliance management.
6. Implement an SCA solution that identifies both security and license compliance issue in code.

Software supply chain management must become a strategic priority for every organization that uses or builds software. Without an SCA solution that provides a complete, accurate SBOM, the benefits of OSS in software development can be overwhelmed by the associated security, license compliance, and IP risks. It's important to identify and mitigate risk by including SCA tools in the application security toolkit.