SPOTLIGHT
Sponsored by: Tidelift

As part of an open source software (OSS) strategy, organizations are increasingly hosting curated OSS package management and artifact repositories internally to mitigate risk and reduce developer friction.

The Importance of a Sound Open Source Supply Chain Management Strategy

June 2022

Written by: Jim Mercer, Research Director, DevOps and DevSecOps

AT A GLANCE

KEY TAKEAWAYS

- Open source software usage has reached a point where it is strategically important for businesses.
- Utilizing curated internal repositories of open source software improves efficiency and reduces security risks.
- Day 2 and ongoing challenges can make it difficult for businesses to build their own curated open source repository.
- A solution for managing the open source software supply chain can optimize application development and remove security, maintenance, and licensing concerns.

Introduction

For modern digital enterprises, application development is very different from traditional methods. Applications are no longer developed from scratch but use a hybrid development approach that includes third-party and open source software (OSS) components integrated with natively developed business logic. Increasingly, application development is taking advantage of OSS components to improve development velocity and leverage the innovation available within the larger OSS community.

The most recent IDC *Accelerated Application Delivery Survey* showed that the percentage of organizations delivering new application features in one to two weeks doubled between 2020 and 2021. Another IDC study showed that by the end of 2022, 15% of applications will be made up of 75–99% OSS (IDC's *Safely and Effectively Building Software Applications with Open Source*, October 2021).

Hidden Unknowns of Open Source

While OSS has a reputation for being "free," organizations need to understand and plan for several hidden costs ahead of using open source software for application development.

Legal and Licensing

There are widely used OSS licenses and thousands of different license combinations within the OSS ecosystem. Potential problems include expired, missing, incompatible, or copyleft licenses. A copyleft, or reciprocal, license requires that any software product embedding the OSS component, even just a few lines out of code, must make its entire source code available for free, along with the rights to modify and distribute it.

Security and Maintenance

Organizations must also consider how OSS embedded throughout their applications is acquired and supported. Most organizations are familiar with consuming software from a COTS vendor where they are protected via a software license agreement with clear indemnification terms. How are your developers acquiring OSS? Can it be trusted? Open source software is available in multiple places across the internet with various levels of reliability and security. Also, with OSS, there is typically no commercial vendor supporting the technology, so organizations are left to rely on the community or do the development work themselves to get needed features, nonfunctional requirements (NFRs), and long-term maintenance.

Because of the imminent threat to the business, organizations need a plan for managing the health and security of their open source software supply chain.

Like software written in-house, OSS can introduce vulnerabilities and security exposures that bad actors can exploit. While OSS does have the community's scrutiny to help build secure code, with OSS embedded in numerous applications, bad actors recognize that adding or finding insecure code in OSS provides the means to attack all the consumers of the OSS code.

White House Executive Order 14208

Executive Order 14208 emphasizes "the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security." Under the executive order, the U.S. National Institute of Standards and Technology (NIST) issued guidance that government agencies and contractors must have a software inventory or software bill of materials (SBOM).

While your organization may not be a U.S. government agency or doing business with the government, the order encourages the private sector to follow suit. As more organizations adopt these standards, they will be expecting the same due diligence from their business partners or vendors.

Civil Penalties

On January 4, 2022, the Federal Trade Commission (FTC) warned companies and their vendors to take reasonable steps to remediate OSS vulnerabilities such as the Log4Shell vulnerability (CVE-2021-44228). In its warning, the FTC states that it intends to use its full legal authority to pursue companies that fail to take reasonable steps to protect consumer data from exposure due to Log4Shell or similar known vulnerabilities in the future. There is already a precedent for this, as Equifax ended up paying $575 million for a data breach caused by an unpatched vulnerability in the OSS Apache Struts.

No Consistent Maintenance and Security Standards Across Open Source Projects

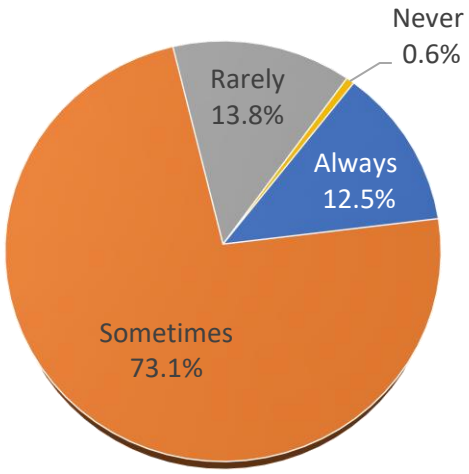
Despite the litany of different projects used for building applications, there are no established standards for building, maintaining, and securing OSS. Essential aspects to evaluate before using OSS include who the project contributors are as well as how many people contribute and their motivation to contribute and maintain the project into the future. How the source code is managed must also be considered, which raises questions such as whether it is adequately secured to resist supply chain attacks, what technologies are in use, and what types of testing are done to ensure code quality. Unfortunately, because many OSS projects are underfunded or rely solely on volunteer contributors, there is a lot of variation in how the projects are maintained.

Benefits

Modern software developers tend to favor OSS over other commercial alternatives. They appreciate having access to an active OSS development community to get assistance for questions and access to the source code itself. Developers may also participate in the community and directly influence which features are added to the OSS component. As Figure 1 shows, an IDC survey of software development and delivery organizations found that 86% of respondents preferred OSS over COTS alternatives. The survey also revealed that in 2022, OSS would be considered strategic for application development.

FIGURE 1: ***Propensity for Using Open Source Software***

Q How often do you try to find open source options over other kinds of software?



n = 161

Source: IDC's DevOps and Accelerated Application Delivery Survey, 2021

The Need for an Open Source Software Management Strategy

Because of the constantly evolving threat landscape, organizations need a plan for managing the health and security of their OSS supply chain. The strategy must be socialized across technical and business stakeholders to get buy-in and should include organizational guidelines for OSS consumption, participation in the OSS community, and standards for security due diligence. Corporate OSS usage, goals, and acceptable risk should be considered part of this effort.

Open Source Program Office

As more businesses adopt OSS, an open source program office (OSPO) can help establish standards for OSS use. Typically, an OSPO is tasked with taking ownership of the OSS strategy and will attempt to align OSS usage and participation with the business strategy and higher-level objectives and key results (OKRs).

An OSPO can define policies around how the organization can and should engage with the OSS community. Such policies may include creating a blueprint for how the organization engages with the OSS community intentionally and ethically to provide additional value to OSS project maintainers and the organization. These policies could also determine how developers access and consume OSS for inclusion in business applications and developer tooling.

Open Source Community Engagement

Most organizations use numerous OSS components across their application portfolios, so they need to be selective about which OSS projects to get involved in. For essential projects with penetration across the application portfolio, it behooves organizations to ensure they have a seat at the table and have a voice regarding project direction and governance. It may be helpful to consider ways to compensate maintainers for their work on selected OSS projects.

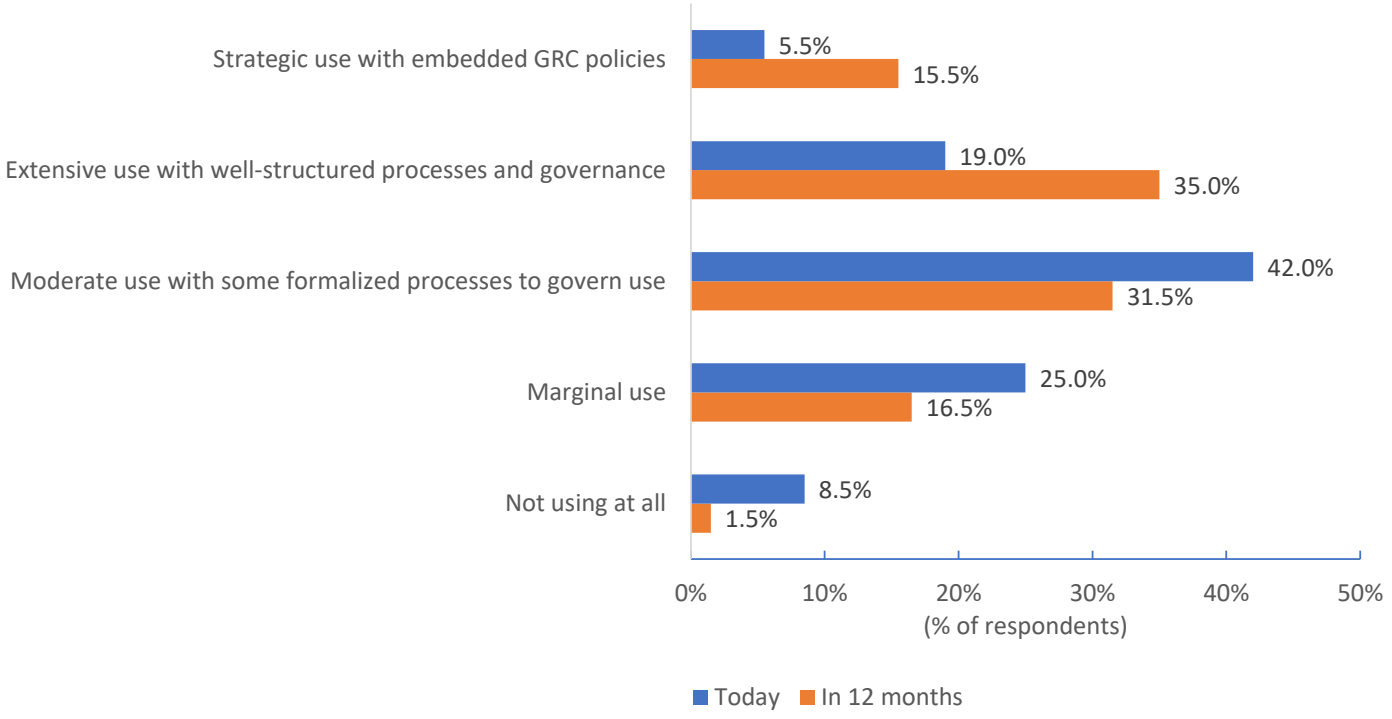
Trends

Many organizations are beginning to realize that how and where their developers access OSS can create process friction and add risk to the business. The Cloud Native Computing Foundation (CNCF) recently released a *Software Supply Chain Best Practices* document that stated, "Organizations should host their own package managers and artefact repositories and restrict build machines to pull from only those sources." The risk of importing vulnerabilities into applications and the wide variety and scope of OSS used in most organizations has seeded the need for internally curated repositories of OSS components.

Figure 2 illustrates how modern digital organizations are gravitating toward creating internal OSS repositories for their application development teams. Internally curated OSS repositories enable organizations to host private package and artifact repositories providing their application development teams with a sanctioned source of OSS components.

FIGURE 2: ***The Digital Enterprise Is Gravitating Toward Internally Curated OSS Repositories***

Q Please assess which of the following statements best describes your use of internally curated open source repositories today and in 12 months.



n = 200

Source: IDC's U.S. Accelerated Application Delivery Survey, January 2022

Managing Open Source at Scale

The initiative of building an internally curated OSS repository may seem feasible initially, but it can quickly become untenable as OSS coverage expands. Common problems include the following:

- **Staffing the team with enough OSS knowledgeable engineers.** By tying up technical resources in assembling and maintaining an internally curated OSS repository, organizations incur an expensive opportunity cost because these resources are scarce and could be working on other projects.
- **Decision making surrounding which component and which versions should be used.** Determining what should and should not be in the repository becomes more complex as different teams may want to consume the same OSS component at different version levels.
- **Tracking OSS vulnerabilities.** In a recent vulnerability report by Risk Based Security, the company that produces the popular VulnDB vulnerability database, 28,695 vulnerabilities were disclosed in 2021, the highest number ever recorded.
- **Insight into OSS projects.** There are too many OSS projects and communities for organizations to monitor effectively. The bad actors are attacking OSS projects and using techniques such as dependency confusion, typosquatting, and ChainJacking to infiltrate the supply chain.

Considering Tidelift

Tidelift cofounders Donald Fischer, Havoc Pennington, Luis Villa, and Jeremy Katz come from OSS lineage and understand the benefits and challenges. Founded in 2017, Tidelift states that it is on a mission to make OSS work better — for everyone. Through its subscription, the company provides the tools, data, and strategies driving an inclusive and organizationwide approach to improving the health and security of the OSS supply chain.

Tidelift recognizes that OSS maintainers play a critical role in the health and security of the OSS supply chain. The company is committed to partnering with OSS maintainers by paying them to ensure OSS components adhere to enterprise-level security, maintenance, and licensing requirements now and into the future. This partnership helps ensure that the OSS on which organizations rely is secure and meets enterprise software quality standards. Tidelift funds this equitable approach, and each customer increases the monthly earnings of maintainers for all the OSS packages they use with no ceiling to the amount maintainers can make.

The Tidelift Subscription enables organizations to do the following:

- Remove obstacles that slow down application development
  - Improve decision making with contextually relevant, maintainer-originated data made available directly in the software development life cycle
  - Define a repository of pre-vetted, approved OSS components that reduce duplicative work and accelerate the development
  - Reduce time to approve new components with a streamlined process integrated into existing workflows

- Identify and remove security-, maintenance-, and licensing-related risk
  - Analyze and document a continuously updated SBOM
  - Assess application risk against OSS components evaluated by Tidelift
  - Design and implement a centralized approach to assessing and curating OSS components
  - Codify and enforce consistent standards and policies across the organization
  - Reduce the need for developers to evaluate raw dependency information while helping shorten the time to identify, assess, and resolve issues by providing validated recommendations on how to resolve issues

Challenges

Tidelift is an early mover in the OSS management space and could potentially face the following challenges:

- **Tidelift can't account for and vet every OSS project — there are too many projects.** Attempting to support every OSS project arbitrarily is a "boil the ocean" approach. Tidelift appears to be focusing on widely accepted projects and growing its catalog of OSS based on customer demand; since its inception, the company has increased the catalog of OSS projects significantly. With Tidelift, organizations can grow their custom OSS repositories over time as their OSS usage grows — adding more tools to the application development toolbox. For application developers looking for specific functionality, the current Tidelift catalog of OSS components offers a variety of options.
- **Although the business model is new and innovative, it has not been proven out over a sustained period.** While the model is unique, and there are growing pains, it has also enabled Tidelift to grow into a new space not already crowded with staunch competitors. While there are some different OSS management options (*IDC Market Glance: DevSecOps, 1Q22*, February 2022), Tidelift competitors reportedly do not offer the same support options and do not support the larger OSS community by paying OSS project maintainers.
- **Given the success of Tidelift and the increased use of OSS, a larger competitor could acquire the company.** If this were to happen, the acquiring company would likely do so to invest in the Tidelift business and provide more opportunities for growing the OSS offering. As Tidelift grows its customer base, this is certainly a possibility. Still, it is sheer speculation, and it is a risk in doing business with any company (IDC's *Decoding DevOps Market Merger and Acquisition Activity, 2011–2021,* April 2022).

Conclusion

As part of the modern digital enterprise, OSS is not just for application developers; it is critical to business success and must be managed like any other business asset. As OSS usage grows across the enterprise, decisions about when and where to use it are strategic to the business and should not be left to individual application developers or DevOps teams. Therefore, organizations must build a business strategy around OSS to reduce organizational risk and realize maximum benefits. Many organizations are now starting to create an OSPO to help guide their OSS strategy and consider how they want to engage with the OSS community.

As part of an OSS strategy, organizations are increasingly hosting curated OSS package management and artifact repositories internally to mitigate risk and reduce developer friction. Initially, this effort can seem straightforward, but it can quickly become untenable as OSS projects, versions, and coverage expand across the application portfolio.

Organizations exploring or composing an internally curated OSS artifact repository might consider the Tidelift Subscription as a do-it-yourself alternative. When considering the ongoing operational cost of a self-managed OSS repository, they should keep in mind that a management solution, such as Tidelift, can enable more efficient use of OSS while reducing risk to the business.

About the Analyst

Jim Mercer, *Research Director, DevOps and DevSecOps*

Jim Mercer is a Research Director within IDC's DevOps Solutions research practice. In this role, he is responsible for researching, writing, and advising clients on the fast-evolving DevOps market. Mr. Mercer's core research includes topics such as rapid enterprise application development, modern microservice-based packaging, application security, and automated deployment and life-cycle/management strategies as applied to a DevOps practice.

MESSAGE FROM THE SPONSOR

More About Tidelift

Tidelift helps organizations effectively manage the open source behind modern applications. The Tidelift Subscription delivers the tools, data, and strategies powering an inclusive and organization-wide approach to improving the health and security of the open-source software supply chain. Tidelift enables organizations to move fast and stay safe when building applications with open source, so they can create more incredible software even faster.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2022 IDC. Reproduction without written permission is completely forbidden.