The Tidelift guide to managed open source

How to develop an effective strategy for maintaining the health of your organization’s open source supply chain

February 2021
What you’ll learn in this guide

This guide explains how to develop a managed open source strategy and help your organization cut costs, accelerate development, and reduce risk when using open source to develop applications.

01 Introduction

02 Managed open source

03 The Tidelift approach to managing open source

04 How to get started
INTRODUCTION

Open source is amazing.
But it has some issues too.
Open source has become the modern application development platform.

Across enterprises and industries, more than 90% of professional applications today are created using open source components. They provide an essential boost to help you develop your app more quickly, but commonly bring with them hundreds of dependencies on other projects and libraries. Manage your dependencies well and your app will perform better while becoming more stable and secure—freeing your developers to focus on creating new functionality.

Source: 2018 Tidelift professional open source survey
Most applications are built on a foundation of 70% or more open source code.

- **20%**: Your custom application code/business logic
  - Top layer of your app, your job to maintain
- **70%**: Open source application components
  - Examples: Babel, Vue.js, Gulp, Material-UI, Fabric, Celery, Jekyll, Active Admin
- **10%**: Commodity infrastructure
  - Examples: Linux, Kubernetes, MongoDB, Docker
  - Maintained by big vendors or cloud providers

Most of your app, but no one’s job to maintain.
Developers love open source for its many benefits

- Makes them more productive
- Speeds up development and deployment time
- Reduces development costs

But as more open source components are introduced, it becomes difficult for organizations to keep up and ensure components are secure and well maintained.

Source: Tidelift open source survey January 2019
Open source-related issues can slow down the development process

Organizations often don’t have a good strategy for addressing these issues efficiently and consistently.

Who can tell me if it is OK to use this package?

Has anyone looked at the license terms?

Is it secure and actively maintained? And if so, by whom?
Software supply chain attacks are increasing. The SolarWinds breach is the latest example of a disturbing trend impacting all software—open source is not immune.

It used to be that the only people thinking about the software supply chain were CIOs and industry analysts. Today—thanks to the breaches that impacted SolarWinds, JetBrains, and all of their customers around the world—these words have found their way to the front page of the New York Times and into tense boardroom conversations.

And unpaid software maintainers often burn out or move onto other projects, leaving critical packages unmaintained. A surprising number of widely used open source packages—between 10 and 20% by some measures—have absolutely no one keeping them maintained. Ghosted and under-maintained packages exist because their creators don't have the time and incentive to keep them up to commercial standards.
The three biggest management issues:

1. **Maintenance**
   First, development teams need guarantees that the packages they use will continue to be maintained into the future. Because if they choose a package that ends up unmaintained, they know they’ll be on the hook to maintain it.

2. **Security**
   Managers live in existential fear of security issues that could put the company at risk.

3. **Licensing**
   And teams also don’t usually have lawyers on staff to sort through the complicated issues surrounding open source licenses.

*Source: Tidelift 2019 Managed open source survey*
Unmanaged open source drains productivity

Most development teams regularly face challenges related to poorly maintained open source components.

Whether it is bugs or security issues related to an unmaintained dependency, or issues caused by missing or unreliable maintainers, most development teams are familiar with the challenges caused by lack of maintenance. And moving to new major versions of components or dealing with breaking changes also cause painful maintenance headaches.

Source: Tidelift 2019 Managed open source survey
Enterprise architecture and technology innovation leaders, including CIOs and CTOs, driving business transformation through technology innovation should: tackle open source as an inevitable investment that, by being properly managed, will yield considerable innovation, total cost of ownership (TCO) and business value benefits. When unmanaged, these same OSS technologies will instead introduce considerable technical, security and legal risks to the enterprise.

Gartner, “What Innovation Leaders Must Know About Open-Source Software,” Arun Chandrasekaran, Mark Driver, 26 August 2019
Managing open source takes time

There’s a saying, “Open source is free, if your time is worth nothing.”

Developers spend an average of nearly 20% of their time on code maintenance, with more than 25% of that time devoted to maintaining their applications’ open source dependencies.

And less than one-third of their time is actually spent writing code!

The biggest organizations are particularly weighed down by open source-related maintenance. Teams with more than 500 developers spend more than one-third of their code maintenance time wrangling open source dependencies.

Source: Tidelift 2019 Managed open source survey
To manage and mitigate the risk of OSS, security and risk management leaders responsible for the security of applications and data must harden the software supply chain to prevent the introduction of vulnerable, malicious or inappropriately licensed software. This can best be accomplished through the creation of an internal repository containing vetted code or artifacts approved for use by developers.

Many teams have little confidence in current open source management practices.

And even more interesting, confidence in an organization’s open source practices declines as the size of the organization grows.

Thirty-nine percent of organizations are not very or not at all confident that their open source components are up to date, secure, and well maintained, while only 16% are extremely confident. To put these findings in another light, imagine if you asked technologists this very same question for any proprietary software product they buy today. If only 16% of respondents said they were extremely confident that this product was up-to-date, secure, and well maintained, how successful do you think that product would be?

When it comes to the open source building blocks at the heart of our organizations’ applications, we should expect no less. We need to ensure that more organizations are extremely confident in the health and security of these critical open source components.

Source: Tidelift 2020 Managed open source survey
The Tidelift Subscription

A comprehensive way for organizations to efficiently manage open source.

Reduce the complexity of managing open source components, while keeping them safe and up to date with help from Tidelift and our growing network of partnered maintainers.

**TOOLS**

We provide the tools to curate, track, and manage catalogs of open source components and the policies that govern them. We also integrate seamlessly with your existing source code and repository management solutions like GitHub, GitLab, and JFrog Artifactory.

**MANAGEMENT**

We research and advise you on how to resolve security, maintenance, and licensing issues. Use Tidelift-managed catalogs as a head start for your organization's paved path and keep your developers moving fast and staying safe.

**MAINTENANCE**

We partner with a large and fast-growing network of open source maintainers who create and maintain the dependencies you use every day, paying them to keep their code secure and up to date—now and into the future.
How organizations manage open source today

Over the past few years, we’ve talked to hundreds of organizations about how they manage their open source. Most of them fall along a spectrum between one of these two extremes.

**Distributed approach**

Many organizations’ development teams are permitted to bring in new components on their own to speed their work. If scanning tools are used to monitor open source security and licensing, the results are often ignored.

- **Upside:** no roadblocks, developers can build and deploy quickly
- **Downside:** creates possibility for maintenance and security nightmares

**Centralized approach**

Other organizations, often in risk-averse industries such as financial services, tightly control open source usage. Scanning tools block deployments until developers address security, license, or other concerns, which they can't always do without substantial rework.

- **Upside:** reduce risk, avoid becoming the next Equifax
- **Downside:** hard to move quickly and developers are frustrated
A strategic way for organizations to consistently manage, secure, and maintain the health of their open source supply chain.
Rather than choose one approach over the other, how can you get both at once?

That’s where a managed open source strategy comes in.
Managed open source is a strategic way for organizations to consistently manage, secure, and maintain the health of their open source supply chain.

Development teams need ready access to open source components to build their applications so they can continue to develop applications quickly. Meanwhile the organization needs to avoid security, maintenance, and licensing-related risk.

Rather than falling into the trap of choosing to move fast or stay safe, how can an organization do both at once?

An ideal solution would:

- **Include the tools** that help your organization manage those sets of components proactively as internal policies/standards and open source software evolves.
- **Integrate** with your build chain and minimize the disruption of your existing processes.
- **Incentivize** the open source software community to continue to maintain and improve the packages your business depends on.
- **Provide a set of “known good” dependencies** for each of the major frameworks.
How do large tech firms manage open source?

They create a “paved path”

➢ Rather than having developers choose packages individually, they establish a library of pre-vetted, known-good open source package releases.
➢ Developers can use these without fear of late-in-the-game deployment blockers.
➢ Vulnerabilities and license concerns can be reviewed centrally, and addressed for the entire organization at once.

But this approach is expensive to build and maintain, which is why only the largest companies have historically tackled it.
03
THE TIDELIFT APPROACH TO MANAGING OPEN SOURCE

A complete solution for managing, securing, and maintaining the health of your open source supply chain. Create, track, and manage customizable catalogs of known-good, proactively maintained open source components.
Open source management tools

The Tidelift Subscription includes all of the tools you need to efficiently track and manage open source across the organization.

A PAVED PATH
Accelerate development by creating catalogs of known-good, proactively maintained components your developers can draw from safely.

CLEAR POLICIES
Automatically enforce standards like your organization’s license policy early in the development lifecycle.

AN INTEGRATED EXPERIENCE
Tidelift integrates with your existing source code and repository management tools so developers don’t need to change their workflow.
Tidelift-managed catalogs

Get a head start on building a paved path for your organization’s developers with our Tidelift-managed catalogs of known-good, proactively maintained open source components covering the language frameworks you use every day.

Check out featured catalogs: https://tidelift.com/catalogs
Backed by maintainers

Tidelift partners directly with the independent maintainers behind thousands of open source projects—with more added every day.

We pay the maintainers to keep their projects enterprise-ready, meeting clearly defined security, licensing, and maintenance standards.

The more subscribers using a project, the more its maintainers get paid. Which means they can dedicate even more time to maintenance and security tasks, while continuing to invest in making their projects even better.

"Tidelift has a really interesting approach to funding open source work. It’s a pretty simple concept: maintainers get paid and the organizations who use their projects get the support and dependability they need in return."

Evan You, Vue.js creator (JavaScript)

"Tidelift has a solution for those companies that would otherwise have to pay many open source projects small amounts each year."

Roel Spilker, Project Lombok (Java)

"Tidelift formalizing a lot of the project minutiae is incredibly helpful—things we should do but often don’t, because there are other things to be done."

Alex Clark, Pillow (Python)
The managed open source journey

As your organization moves further in implementing a managed open source strategy, the benefits will continue to multiply.

<table>
<thead>
<tr>
<th>UNDERSTAND</th>
<th>BUILD</th>
<th>AMPLIFY</th>
<th>EXCEL</th>
</tr>
</thead>
<tbody>
<tr>
<td>● Inventory open source components</td>
<td>● Curate a paved path of approved components</td>
<td>● Add more developers and projects</td>
<td>● Best-in-class practices for managing open source in place</td>
</tr>
<tr>
<td>● Define standards around security, maintenance, and licensing</td>
<td>● Implement standards and policies</td>
<td>● Alert developers when they leave the paved path</td>
<td>● Open source components proactively maintained and secured</td>
</tr>
<tr>
<td></td>
<td>● Choose test projects and validate prototype</td>
<td>● Expand catalogs of approved components</td>
<td>● Clear standards and policies working across the organization</td>
</tr>
</tbody>
</table>

- **TIME**
  - Improve visibility into open source usage
  - Establish a paved path for developers
  - Move fast and stay safe
  - Open source becomes a competitive advantage

- **IMPACT**
  - Establish a paved path for developers
  - Move fast and stay safe
  - Open source becomes a competitive advantage
Understand open source usage

Get a unified view of the open source you use by generating a bill of materials along with the associated metadata for each project containing open source packages.
Define a paved path for developers

Create catalogs of known-good components that are approved for use in your organization and customize the security, maintenance, and licensing standards.
Get a head start with Tidelift-managed catalogs

Begin with our catalogs of proactively maintained components and backed by maintainers, and import them into your own custom catalogs.
Integrate into your CI/CD pipeline

Ensure only approved components make it into production and give developers guidance on what they should use instead if a build fails.
Benefits across the organization

Get your internal stakeholders aligned around the benefits of having a managed open source strategy in place.

**MANAGER**

*Increase development velocity*

Build with safe, approved, and compliant packages from the start to speed up development and reduce technical debt.

**INFOSEC**

*Establish a paved path for developers*

Get a single place to define, review, and enforce policies around security vulnerabilities in open source components.

**DEVELOPER**

*Move fast and avoid rework*

Eliminate late-breaking surprises that slow down development by using pre-approved, known-good open source components.

**LEGAL**

*Reduce open source-related risk*

Get a single place to define, review, and enforce license policies and get indemnification to protect against licensing-related risk.

Get your internal stakeholders aligned around the benefits of having a managed open source strategy in place.
HOW TO GET STARTED

Ready to design a managed open source strategy for your organization? Here are some resources that can help.
Watch a demo of the Tidelift Subscription.

See how the Tidelift Subscription can help you move fast and stay safe with catalogs of known-good open source components to use when building your apps.

➔ To watch the demo, go here: https://tidelift.com/subscription/watch-demo
Continue your research

Visit our resource library.

Learn more about how to develop an effective strategy for managing open source through our videos and webinars. You can also get additional information about how other organizations like yours tackle open source-related issues with our survey reports.

Find some great places to start in our resource library:

tidelift.com/about/resources
About Tidelift

Tidelift helps organizations effectively manage the open source behind modern applications.

Through the Tidelift Subscription, the company delivers a comprehensive management solution, including the tools to create customizable catalogs of known-good, proactively maintained components backed by Tidelift and its open source maintainer partners.

Tidelift enables organizations to accelerate development and reduce risk when building applications with open source, so they can create even more incredible software, even faster.