THE TIDELIFT GUIDE TO MANAGING OPEN SOURCE
for application development teams

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

January 2022
WHAT'S COVERED IN THIS GUIDE

The guide explains how to develop an effective strategy to help your organization move fast and stay safe when developing applications with open source.

1  INTRODUCTION
2  THE TIDELIFT APPROACH TO MANAGING OPEN SOURCE
3  GETTING STARTED
INTRODUCTION
OPEN SOURCE IS THE MODERN APPLICATION DEVELOPMENT PLATFORM

Today, when it comes to building applications, open source is everywhere.

It gives anyone trying to innovate with software a head start, with billions of lines of code, freely available, developed and shared through an open community of creators, collaborators, and maintainers.

Because of this, most modern applications are built using open source, and in many cases it makes up more than 70% of the code.

Source: 2018 Tidelift open source survey

- 92% of modern applications contain open source components
- 20% Your custom application code/business logic
- 70% Open source application components
- 10% Commodity infrastructure
WHY DEVELOPERS LOVE OPEN SOURCE

In a recent Tidelift survey, we asked application developers to tell us why they use open source. Here were the top three benefits they shared.

- Makes them more productive
- Speeds up development and deployment time
- Reduces development costs
Despite its many benefits,

DEVELOPING APPLICATIONS WITH OPEN SOURCE CAN BE CHALLENGING.
INTRODUCTION

Challenge #1

OPEN SOURCE PROJECTS ARE OFTEN DEVELOPED AND MAINTAINED BY VOLUNTEERS

Most open source projects start as passion projects or are designed to directly address a gap identified by their creator. Yet there are not many incentives for the creator to continue maintaining the code over time, beyond their personal investment in the project. What’s more, even when these projects are actively maintained, there is no common standard for how they should be kept secure and up to date.
This means enterprises hoping to make decisions about components they would like to use for years into the future are left to make educated guesses as to which projects will continue to be maintained and which will not. When they guess incorrectly, the organization is often left on the hook to maintain a project on their own that has become a critical part of their application or—worse—let it fall into disrepair and put the organization at risk.

This is where open source creates difficult and time-consuming security and maintenance challenges for organizations, who may not have the time or in-house expertise to identify and remediate issues with the components they use.
Challenge #2

ORGANIZATIONS GENERALLY HAVE LITTLE CONFIDENCE IN THEIR OPEN SOURCE MANAGEMENT PRACTICES

Given these issues, it is no wonder that organizations have concerns about how well they are managing open source today. In a recent survey, we found that confidence in an organization’s open source practices declines as the size of the organization grows.

In organizations with more than 10,000 employees, we found that 39% 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 developers this very same question for any commercial software product they use. Can you imagine a commercial product where only 16% of respondents were extremely confident in how secure, up-to-date, and well maintained it is? How many organizations would want to use that kind of product?

When it comes to the open source building blocks at the heart of your organizations’ applications, you want to have confidence these critical components are healthy and secure, and will continue to stay that way into the future.

Source: Tidelift 2020 managed open source survey
Challenge #3
OPEN SOURCE-RELATED ISSUES CAN SLOW DOWN DEVELOPMENT TEAMS

Organizations typically lack a consistent and centralized approach for managing open source standards and usage policies. This leaves individual developers to address questions such as:

- Whose job is it to determine if a component is OK to use?
- Does it meet our security standards?
- Is there someone actively maintaining it?
- Is there a particular version that we should be using?
- What upstream transitive dependencies does the component have? Who is responsible for maintaining those dependencies?
- Are there specific license terms that would prevent us from using it?

Not having accessible answers to questions like these slows down the development process and often leads to open source sprawl within the organization.
WHAT ARE THE BARRIERS TO ORGANIZATIONS INCREASING OPEN SOURCE USAGE?

Tidelift’s 2019 managed open source survey showed that the biggest obstacles standing in the way of organizations increasing their use of open source are:

- **Maintenance**: Risk about how well the package will be maintained (76%)
- **Licensing**: Concern over licensing/compliance (64%)
- **Security**: Identifying/remediating security vulnerabilities (63%

Based on 320 responses.

**Maintenance**

Development teams need confidence that the components they use will continue to be maintained into the future. If they choose a package that ends up unmaintained, they know they’ll either need to rip and replace or take on the burden of maintaining it themselves.

**Licensing**

Not all open source code is licensed the same way. In fact, there are a dizzying number of license types, with varying sets of terms. Application development teams don’t always have access to experts who can sort through complex licensing issues or help determine whether the organization is in compliance with the license terms.

**Security**

Security vulnerabilities represent an existential threat to all organizations, where high profile attacks like Log4Shell and the ones that impacted SolarWinds, Equifax and their customers are the nightmare scenarios every organization wants to avoid. So application development teams want to have confidence that the open source components they choose will not put the organization or its customers at risk.
INTRODUCTION

THE RISE OF SOFTWARE SUPPLY CHAIN ATTACKS

Until recently, the term “software supply chain” was rarely uttered outside of the offices of CIOs and senior government officials. But in the wake of high profile attacks like the one that impacted the open source Java logging component Log4j, times have changed. Now, software supply chain security is the subject of terse boardroom conversations and New York Times headlines.

While not all software supply chain attacks involve open source (SolarWinds, for example was not open source), open source is not immune from such attacks either. With the Log4Shell or node.js event-stream exploits, the fact that the compromised component had been downloaded and incorporated into hundreds or millions of applications vastly increased the scale of the potential impact.

“The risks associated with a supply chain attack have never been higher, due to new types of attacks, growing public awareness of the threats, and increased oversight from regulators. Meanwhile, attackers have more resources and tools at their disposal than ever before, creating a perfect storm.”

CSO MAGAZINE, OCTOBER 2020
INTRODUCTION

GOVERNMENTS AROUND THE WORLD ARE MAKING SOFTWARE SECURITY A TOP PRIORITY

In 2021, the U.S. White House released cybersecurity executive order 14028, an attempt by the United States government to strengthen its own cybersecurity defenses while also using its purchasing power to positively impact how cybersecurity is addressed around the world.

This executive order forces a higher standard of cybersecurity for any organization selling software to the federal government, which in turn makes it the de-facto global standard for all software moving forward.

Source: The Washington Post

National Security

Biden signs executive order designed to strengthen federal digital defenses

“In so many areas of computer security, what the federal government does first, the private sector follows,” said Schwartz, managing director of cybersecurity at Venable, a law firm. “What the federal government is requiring here likely will become the standard for all software moving forward—not just in the United States but internationally.”

Source: The Washington Post
DESPITE THESE ISSUES, OPEN SOURCE IS AMAZING. IT IS HERE TO STAY.

Organizations just need a better strategy for managing it.
A BETTER APPROACH TO MANAGING OPEN SOURCE FOR APPLICATION DEVELOPMENT TEAMS

The benefits of developing applications with open source are too pronounced to ignore, and organizations that do not take advantage of these benefits will be left behind by those that do.

The challenge for application development leaders is ensuring they are taking full advantage of all the innovative potential of open source in a way that does not impede developers or put the organization at risk.

The best way to get the most of open source? Ensure the organization has a comprehensive strategy for managing open source in place.
SO HOW ARE MOST ORGANIZATIONS MANAGING OPEN SOURCE TODAY?
When it comes to their strategy for managing open source, most organizations fall somewhere on the spectrum from a distributed approach which helps developers move fast (but increases the potential for maintenance or security nightmares) and a centralized approach, which helps organizations minimize open source risks and stay safe (but slows down developers with added bureaucracy).

**DISTRIBUTED APPROACH**
Developers on each team bring in new components on their own. If scanning tools are being used, the results are often ignored.

**Upside:** no roadblocks, devs can build and deploy quickly

**Downside:** creates possibility for maintenance and security nightmares

**CENTRALIZED APPROACH**
Organization tightly controls open source usage to avoid risk. Scanning tools block deployments until developers address concerns, which they can’t always do.

**Upside:** reduce risk, avoid becoming next Equifax

**Downside:** hard to move quickly and developers are frustrated
It begs the question: is there an approach to managing open source that provides you the best of both worlds? Where the organization can **MOVE FAST AND STAY SAFE?**
WHAT APPROACH SHOULD ORGANIZATIONS USE TO MANAGE OPEN SOURCE?

Implementing a comprehensive approach to managing their open source supply chain is challenging for most organizations and can’t be done overnight. Instead, organizations should look to systematically improve their strategy and practices over time. As an organization builds its open source management practice, they should follow the path described over the following pages.
1. UNDERSTAND

Organizations should begin by getting better visibility into the open source components already in use. This often involves creating a software bill of materials (SBOM) to track open source components, versions, and upstream dependencies across the organization.

GOAL
Increase visibility into open source usage.
Next, organizations should define standards and policies around security, maintenance, and licensing for open source. They should assess and improve team practices in an effort to reduce open source-related risk and improve overall application health.

**GOAL**
Define a scalable system for managing open source.
At this stage, organizations can start paying down technical debt by eliminating open source components that do not align with the standards and policies that have been implemented.

At the same time, they can start proactively pre-vetting and approving new open source components based on their standards and policies, building a “paved path” for developers, a repository of pre-vetted, approved components that developers can use without fear of late in the game deployment blockers.

GOAL
Move fast and stay safe.
4. TRANSFORM

Finally, the organization is able to manage open source at scale with all development teams aligning their applications to approved repositories and centrally managing and vetting requests for new components. The organization can take advantage of all of the innovative potential of open source fueling innovation and transformation.

GOAL
Gain competitive advantage from open source.
INTRODUCTION

HOW DO THE LARGEST TECH COMPANIES MANAGE OPEN SOURCE?

1. They create a paved path of approved components

2. They centralize open source management

3. They grow a repository of approved components over time

This is also the approach recommended by top analyst firms. It improves an organization’s efficiency when developing with open source. But it has historically been time consuming and expensive to build, staff, and maintain, which is why only the largest organizations attempt it.

Let’s learn more about how this approach works:
CREATE A PAVED PATH

Build a repository of vetted and pre-approved open source components and release versions. Developers who stay on the paved path can move quickly and avoid last-minute blockers from scanning tools.
Set organization-wide security, maintenance, and licensing policies for open source. New component and version requests are reviewed centrally, for the entire organization at once, so individual developers don’t need to become security and licensing experts.
Once components are approved, they are added to the paved path. As this repository of pre-vetted components grows over time, development teams become more efficient because they have a larger set of pre-approved components to draw from.
“Organizations with a low appetite for risk often wish to exert a greater degree of control over the use of OSS in applications. In these cases, a typical response is to create a repository of ‘approved’ open-source packages. Developers are free to incorporate any software contained in the repository, but other packages must go through a review and approval process. This approach presumes the availability of resources to review suggested editions and maintain the currency of the ‘approved’ packages in the repository.”

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.
THE TIDELIFT APPROACH TO MANAGING OPEN SOURCE
TIDELIFT HELPS ORGANIZATIONS EFFECTIVELY MANAGE THE OPEN SOURCE BEHIND MODERN APPLICATIONS.

We provide a comprehensive approach to help application development teams improve the health and security of their software supply chain so they can move fast and stay safe when building applications with open source.
THE TIDELIFT APPROACH TO MANAGING OPEN SOURCE

THE TIDELIFT SUBSCRIPTION

A better approach for improving the health and security of the open source software supply chain.

Tidelift helps organizations streamline the application development process by removing obstacles that slow down developers while identifying and minimizing open source-related risk—with help from Tidelift and our growing network of partnered maintainers.
The Tidelift Subscription consists of **THREE CORE COMPONENTS:**

1. Open source management tools
2. Tidelift catalog
3. Custom catalogs
OPEN SOURCE MANAGEMENT TOOLS

These tools provide visibility into the open source components being used, as well as the ability to understand and map upstream transitive dependencies. Users can generate software bills of materials (SBOMs) to continuously track all the open source packages used in their applications. SBOMs also provide insights such as:

- release and license information
- upstream dependency chain and provenance information
- package evaluation and approval status

Additionally, users get access to security vulnerability, licensing, and maintenance issues for all the packages in the SBOM, as well as the ability to monitor, review, and address new dependency information.
TIDELIFT CATALOG

This is Tidelift’s version of the paved path that an organization can use out-of-the-box. The Tidelift catalog is integrated into the subscription and can be accessed by developers via the web user interface or the command line interface. It provides an effective starting point for development teams wanting to build applications using packages that are pre-vetted and approved by Tidelift. Additionally functionality such as verified software package data exchange (SPDX) formatted license data, up-to-date maintenance and vulnerability data, and automated license analysis and policies are also built into the catalog.
CUSTOM CATALOGS

Custom catalogs give teams the ability to start implementing open source usage practices and standards that align with their organization’s strategies, risk appetite, and industry regulations. Using the defined standards and policies, organizations can start evaluating packages in-house, with the goal of creating their own unique paved path of pre-vetted and approved packages for developers to use. Organizations can also track application compliance with internal security, licensing, and maintenance policies. Custom catalogs also provide the ability to track non-public, internally developed (inner-source) packages that are exclusive to the organization. Custom catalogs deliver the ability to really mature and transform an organization’s use of open source software.
WHAT MAKES TIDELIFT DIFFERENT?
A PURPOSE-BUILT APPROACH TO MANAGING OPEN SOURCE

Tidelift provides the tools, data, and strategies that drive an inclusive and organization-wide methodology for improving the health and security of the open source software supply chain. With the Tidelift Subscription organizations can define open source standards and policies that make it easy to provide a paved path of pre-vetted and approved open source projects for developers to use.

With the Tidelift Subscription in place, organizations can enforce the agreed-upon standards and policies in an effort to achieve consistent open source development across the organization, while also enabling educated decision making with contextually relevant data and information. Finally, Tidelift makes it easy to eliminate silos and increase collaboration in an effort to improve the health and safety of the open source software supply chain.
UPSTREAM MAINTAINER PARTNERSHIPS

Tidelift partners directly with maintainers and pays them to ensure the open source software your organization relies on meets enterprise standards now and into the future. As a result, we reduce the need for developers to evaluate raw dependency information on their own, while helping shorten the time to identify, evaluate, and resolve issues by providing validated recommendations on how to resolve issues.

In addition, we also provide tools and practices for maintainers to identify upstream security and maintenance issues in an effort to keep the open source software supply chain secure.
GETTING STARTED
GETTING STARTED

Watch a demo of the Tidelift Subscription
See how the Tidelift Subscription can help your development teams move fast and stay safe by building applications with pre-vetted and approved open source components.

WATCH THE DEMO

Continue learning more
Learn more about developing an effective strategy for managing open source through our guides, videos, and webinars.

VISIT OUR RESOURCE LIBRARY

Get detailed technical information about the Tidelift Subscription.

VISIT OUR TECHNICAL DOCUMENTATION