DECEMBER 2023

TIDELIFT

The guide to managing open source software risk with Tidelift

LEARN HOW TO PROACTIVELY REDUCE RISK, IMPROVE SECURITY, AND USE OPEN SOURCE WITH CONFIDENCE

What's covered in this guide

TIDELIFT

Introduction

The benefits of open source

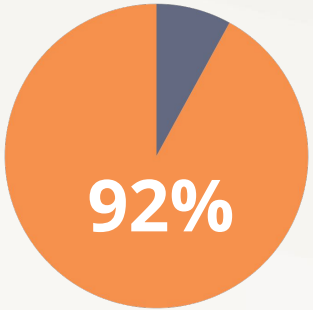
Open source is the modern application development platform

These days, open source is everywhere.

Using open source 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.

Open source helps increase developer productivity, accelerates development and deployment, and reduces application development costs.

However, it comes with hidden costs related to keeping it secure and well maintained.



of applications contain open source components

Open source code makes up 70% or more of the average application

Source: 2018 Tidelift open source survey

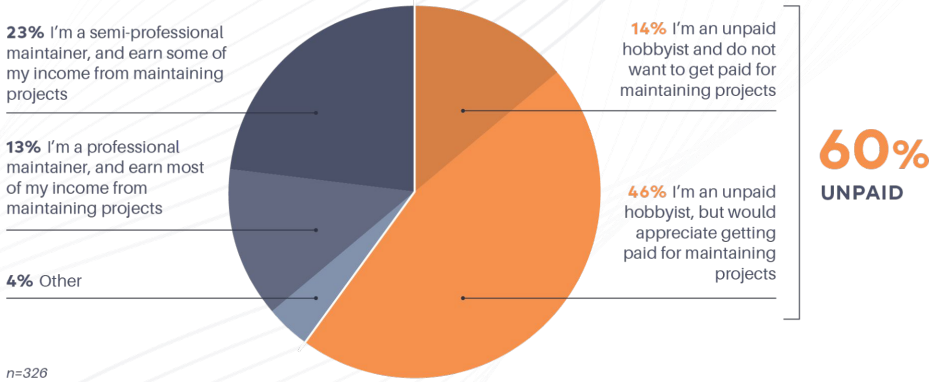
The hidden challenges of open source

60% of open source projects are maintained by unpaid hobbyists. These volunteer maintainers often lack the time and incentives to implement the secure software development practices enterprise users require, not to mention that security and maintenance practices vary widely from project to project.

This in turn forces organizations to take on the responsibility for ensuring their open source software supply chain is secure and well maintained—**extremely research-intensive and time-consuming work.**

60% of maintainers describe themselves as unpaid hobbyists

Which of the following phrases best describes how you approach your role as an open source maintainer?



n=326

Source: 2023 Tidelift maintainer survey

Looking at this through the lens of an open source package maintainer, as Seth Michael Larson, maintainer of urllib3, a popular Python package with billions of downloads a year, put it:

"Being a maintainer of an open source project requires running fast just to stay still. Every project requires security responses with fixes, updates to dependencies, and support for new language versions, features, and platforms. When the amount of work demanded from maintainers becomes too much we lose maintainer time to burnout, disinterest, and frustration."

– Seth Michael Larson, "People in your software supply chain," May 31, 2022

Did you know?

In 2023, **more than three-fifths (61%)** of U.S. businesses have been directly impacted by a software supply chain threat.
(Capterra; Infosecurity Magazine)

TIDELIFT

So, how are most organizations managing open source software risk today?

How are most organizations managing open source software risk today?

Historically, software composition analysis (SCA) tools have been a common way for organizations to manage open source security issues. They are good at identifying known security vulnerabilities and helping organizations respond to them, but are only part of the solution.

To turn analyzing open source into a food metaphor, SCA is strong at showing you when food is spoiled...but you also need a strategy for sourcing better quality food as well.

DON'T EAT SPOILED FOOD

SCA is really good at helping your organization fix known vulnerabilities in open source.

AND

SOURCE BETTER QUALITY FOOD

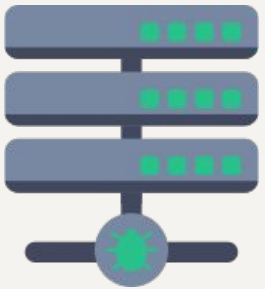
But you also can make active decisions to bring in open source components that are being developed securely in the first place!

Organizations using SCA tools still typically struggle with:

- Too much vulnerability data to digest. In 2022 there were over 17K new vulnerabilities.
- Developers complaining about being slowed down by having to differentiate between real issues and false positives.
- Developers not knowing how to remediate CVEs or how to prioritize which CVEs to address first.
- Vulnerabilities leading to work stoppages and causing rework while development teams are expected to deliver on tight deadlines.

The bottom line:

We are living in an era where reacting to late-stage risk alone is no longer enough to secure your organization's software. By the time an SCA tool has discovered a vulnerability, it's too late because the vulnerability is already in your software development lifecycle. Open source software supply chain threats are much broader than what CVEs tell us. More and more, organizations are starting to recognize the importance of minimizing the likelihood of being exposed to a vulnerability in the first place.



TIDELIFT

How can organizations manage open source software supply chain security even more effectively?

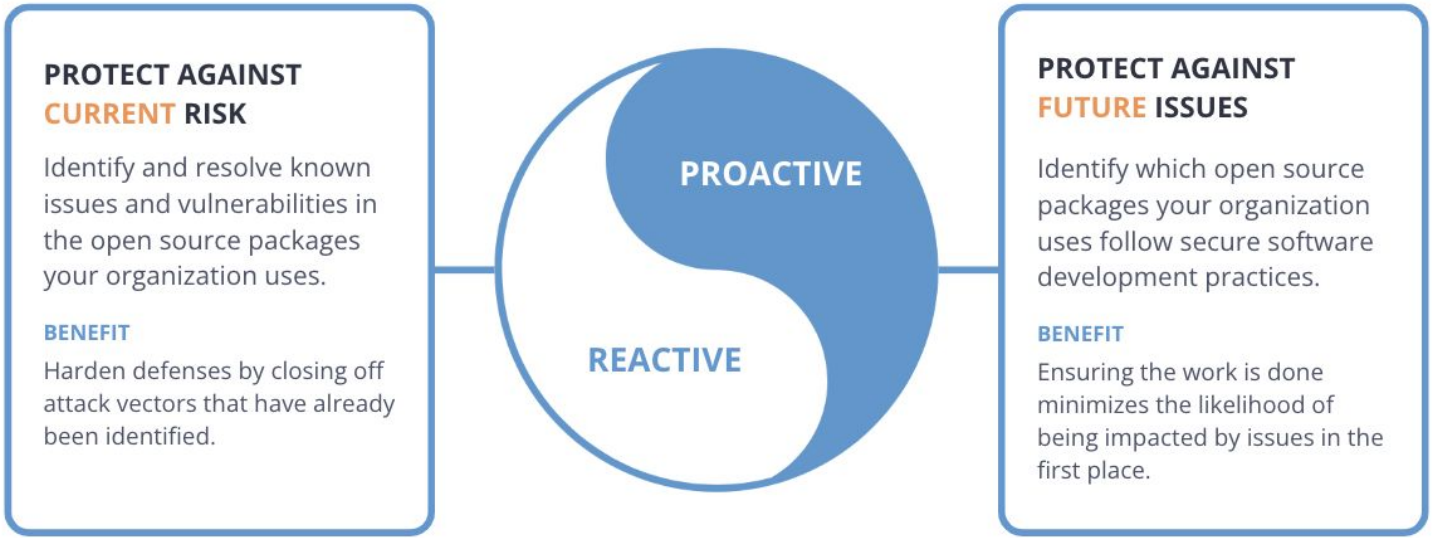
Defense-in-depth

At Tidelift, we recommend organizations take a more holistic, **defense-in-depth approach** to open source software supply chain security that combines reactive tools such as SCA together with a more proactive solution.

SCA tools are very effective at identifying and helping remediate current, known risks and vulnerabilities. This helps you close off already identified attack vectors.

Additionally, you should also implement a proactive approach that helps protect against future issues. This includes ensuring the open source projects your organization uses are developed using secure development practices, so you can minimize the likelihood that issues will impact you in the first place.

Proactive and reactive strategies deployed together can improve the security of your organization's open source software supply chain.



Some examples of proactive decision-making that can help protect your organization against future issues:

- Is the open source software you use deprecated?
- Is the open source software you use still maintained or abandoned?
- Is the open source software you use responsive to security issues?

and more

TIDELIFT

This is where Tidelift comes in

In partnership with paid open source maintainers, Tidelift provides accurate, human-researched, maintainer-validated data about how the open source your organization relies on is secured and maintained, allowing you to make better proactive decisions and manage future risk when using open source.

Tidelift documents the secure development practices of the open source projects organizations rely on most

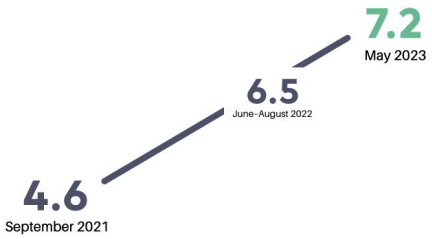
Tidelift pays open source maintainers to ensure their projects follow industry-standard secure software development practices (such as those found in the NIST Secure Software Development Framework and the OpenSSF Scorecards).

Examples of the standards implemented by Tideilift's partnered maintainers:

- Validated license
- Validated versioning scheme
- Release managers reviewed
- Vulnerabilities have document review
- Vulnerabilities have fixed release or documented mitigation available
- 2FA on source repository
- 2FA on package manager
- Documented maintenance plan
- Validated source repository url
- Discoverable security policy

TIDELIFT'S MULTI-YEAR PARTNERSHIP WITH MAINTAINERS HAS INCREASED OVERALL SCORES BY 57%

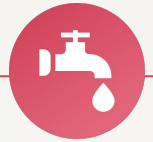
Through a focused effort on scorecards starting in June of 2022 to May 2023, Tidelift increased OpenSSF scorecard scores from an average of 6.5 to 7.2 (n=26), increased maintainer engagement with scorecards, and improved how scoring is assessed.



TIDELIFT

How organizations use Tidelift to manage open source software risk

How organizations use Tidelift



Validated open source security and maintenance data

Use Tidelift's package, release, and vulnerability APIs to give your teams access to a continuously curated stream of validated data about vetted components they need to make intelligent decisions, faster.

Open source management and policy compliance

Create catalogs of vetted, approved open source components that follow secure software development practices, then continuously curate them against the set of organizationally-defined open source policies.

Compliance with mandatory government cybersecurity requirements

For organizations selling software to the U.S. government, get the data you need to attest to the secure development practices of the open source components used in your applications.

Validated open source package intelligence

For organizations that rely heavily on open source software but struggle to understand how specific open source components might make them more susceptible to vulnerabilities and attacks.

BENEFITS

Open source intelligence data at scale.
Tidelift has built a unified, cross-ecosystem data model covering millions of open source packages.

Reduce time spent analyzing packages and make better decisions with first-party data about secure software development practices, release guidance, licensing information, and more.

Data where you need it. Access these insights via APIs, with the flexibility to pull it into your preferred workflows and tools.

Open source management and policy compliance

For organizations that rely heavily on open source software but struggle with a lack of visibility regarding package usage across the organization and have development teams downloading packages that have not been evaluated against organizational risk parameters, adding concerns about open source security risks.

BENEFITS

Improve visibility. Get a complete view of open source in use across the organization, including transitive dependencies, generate up-to-date SBOMs after every build.

Improve decision-making. Make more informed decisions with human- researched, validated, and normalized metadata—and share them across the organization.

Improve management. Centralize open source security, maintenance, and licensing policies and standards while empowering developers to self-serve from catalogs of approved components.

Improve resilience. Validate that the components you use meet industry and government standards—now and into the future.

Compliance with mandatory government cybersecurity requirements

For organizations selling software to the U.S. government that are required to self attest that they follow the secure software development practices outlined in the NIST Secure Software Development Framework (SSDF).

BENEFITS

Tidelift is the only source for first-party attestation data from the maintainers behind thousands of open source packages that go into your software, aligned to the U.S. government's NIST Secure Software Development Framework (SSDF) standards. In addition, we provide:

A standardized attestations report, to be used as evidence that the open source dependencies in your organization's applications follow secure software development best practices.

A solution for dynamically tracking attestations for open source components going into your product, and keeping the attestations current in an automated manner.

TIDELIFT

The Tidelift Subscription

Product capabilities

The Tidelift Subscription provides a proactive approach to reducing risk by helping organizations make better-informed decisions about open source software.

Insights

Proactively evaluate the security, licensing, and maintenance risks of open source software using Tidelift's centralized, structured, and continuously curated database of insights spanning millions of open source packages.

Visibility

Ensure stakeholders are able to respond to issues and vulnerabilities by giving them appropriate visibility around open source software usage across the organization.

Management

Mitigate long-term organizational risk by standardizing open source software management practices and policies across the organization.

INSIGHTS

The easiest way to avoid having to replace problematic open source dependencies is to not bring them in at all.

Organizations rely on Tidelift to assist in reviewing new open source software being considered for use, ensuring it:

- Matches their license policy
- Has a history of responding to security and other issues
- Is actively maintained and receiving fixes
- Has financial support to ensure long-term viability

and more

Tidelift provides a one-stop shop for answering these questions. Open source program offices save the time they would have spent researching, meaning developers can get answers faster, and security and legal departments have peace of mind by proactively reducing risk.

VISIBILITY

Having visibility into the open source software being used across the organization is critical for understanding the impact of a vulnerability and undertaking appropriate remediation efforts in a timely manner.

With Tidelift, organizations can:

- Build a centralized inventory of all the open source packages being used by generating or importing software bills of materials (SBOMs) in CycloneDX and SPDX formats
- Easily implement remediation by mapping how and where a specific package or release came into your software dependency chain
- Prioritize remediation actions by identifying whether a package is being used in a runtime or test environment
- Evaluate dependency information, correctly catalog direct and transitive dependencies, and map how specific dependencies are being pulled into their code

and more

MANAGEMENT

Reviewing new open source packages under consideration to understand their development practices is a good thing. But it's not a one-time solution; it is equally important to monitor the open source components your organization uses in an ongoing manner. Software can be re-licensed, newer versions are constantly being released, maintainers can lose funding to continue maintenance, or can walk away and abandon or deprecate a package at any time.

Tidelift continuously analyzes open source software and keeps you informed of changes as they happen, not months or years later when a latent vulnerability is discovered and no one's there to fix it.

We've built out-of-the-box functionality that automates long term open source management by providing answers such as:

- **Has a previously approved package been exposed to a new vulnerability?**
- **Did an actively maintained package become deprecated, thus introducing new risk vectors?**
- **Are you correctly tracking license information and ensuring that previously reviewed and approved license information has not changed?**
- **Are your developers using older, outdated versions or deprecated packages that might not be supported, or expose you to new vulnerabilities?**

and more

TIDELIFT

It’s time to get proactive about reducing open source security risk

Why now?

Open source changes at a breathtaking rate in modern software development. Development teams make many choices each day about what packages to start or stop using. Impacting these choices are thousands of dependency graphs, where package maintainers are also making choices continuously. New versions ship, security weaknesses emerge, packages are abandoned, and contributors change.

We are living in an era where reacting to late-stage risk alone is no longer enough to secure your organization's software. There are too many vulnerabilities to respond to. Open source software supply chain threats are much broader than what CVEs tell us. And managing all of this at scale is overwhelming.

Tidelift is designed to be your organization’s proactive defense-in-depth strategy for protecting your open source software supply chain. We have built tooling that delivers insights, visibility and management at scale across millions of open source packages.

TIDELIFT

About Tidelift

About Tidelift

Tidelift helps organizations improve the health and security of the open source powering their applications. We partner with leading open source maintainers to provide human-validated data about the secure development practices followed by the world's most critical open source projects. Tidelift enables organizations to use open source with confidence, so they can create more incredible software, even faster.

SELECTED CUSTOMERS

HUGHES An EchoStar Company
BLOOMBERG
AIR FORCE
DARPA
JPL Jet Propulsion Laboratory California Institute of Technology
Fannie Mae
USGS

INVESTORS

FOUNDRY
GENERAL CATALYST
Dorilton Ventures
ae HORIZONX
ATLASSIAN Ventures
CISCO investments
KAISER PERMANENTE
IDC Innovator

Getting started

Watch a demo of the Tidelift Subscription

See how the Tidelift Subscription can help your organization use open source with confidence, so you can create more incredible software, even faster.

WATCH THE DEMO

Visit our resource library

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

EXPLORE OUR RESOURCES

Get detailed technical information about the Tidelift Subscription.

VISIT OUR TECHNICAL DOCUMENTATION

Get in touch

Contact us to schedule a time to chat live and learn more about how Tidelift can help you.

CONTACT US