The Tidelift guide to managing open source

HOW TO DEVELOP AN EFFECTIVE STRATEGY FOR MAXIMIZING THE RESILIENCE OF YOUR ORGANIZATION'S OPEN SOURCE SOFTWARE SUPPLY CHAIN
What’s covered in this guide

Introduction 3
   The benefits of open source 4

The hidden challenges of open source 5
   How should organizations meet these challenges? 10

Continued impact of open source software supply chain attacks 11
   Government response to open source security issues 15
   A call for improved security and maintenance standards 17

How should organizations address these open source-related challenges? 20
   Defense in depth 21
   How Tidelift can help 22
   The Tidelift Subscription 23

The key benefits of the Tidelift Subscription 24
   Maintainer-validated standards 30

Why now? 31

Getting started 33
Introduction
The benefits of open source

OPEN SOURCE IS THE MODERN APPLICATION DEVELOPMENT PLATFORM.

Open source software is an amazing resource and it is nearly impossible for organizations to build applications without incorporating open source into their code. Approximately 92% of applications contain open source components and open source code makes up 70% or more of the average application.

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.

Source: 2018 Tidelift open source survey
The hidden challenges of open source
Open source helps increase developer productivity, accelerates development and deployment, and reduces application development costs.

However, it often comes with hidden security and maintenance costs.

This XKCD cartoon illustrates the two principal challenges organizations face when managing open source:

- Internal open source security and maintenance challenges
- External open source software supply chain resilience challenges

Courtesy of xkcd
Security and maintenance challenges

Most organizations are already aware of the internal security and maintenance challenges that come with using open source.

Some of the questions many organizations struggle to answer include:

- **Whose job is it** to keep the open source components the organization relies on secure, up-to-date, and well maintained?
- **Who is on the hook** to fix issues with these components when they occur?
- **Who makes decisions** about which open source components and versions are approved for use?
- **Who writes fixes** for vulnerabilities flagged by software composition analysis tools if not already available?
In our 2022 open source survey we asked technologists how confident they are in their organizations’ open source management practices.

Only 15% of organizations answered that they were extremely confident about how well they were managing open source security, maintenance, and licensing issues today.

Furthermore, 87% of large organizations reported struggling to make good decisions about which open source components to use.

Source: 2022 Tidelift open source survey
Supply chain resilience challenges

In 2021, Tidelift fielded its first-ever comprehensive survey of open source maintainers. Nearly 400 maintainers responded with thoughts about their contributions, compensation, the open source community, and other key insights. A few important findings:

- **Only 26%** of maintainers reported earning more than $1000 a year. A year.
- **Almost half** (45%) of open source maintainers reported earning nothing for their work.

This means that almost three-fourths of open source maintainers make pizza money or less to keep their projects secure and properly maintained. And it forces organizations to take on these difficult security and maintenance challenges on their own—when they can.

Jim Mercer of IDC perfectly sums up this supply chain resilience challenge in a recent report on open source management best practices:

“Despite the litany of different projects used for building applications, there are no established standards for building, maintaining, and securing OSS. 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.”

IDC, “The Importance of a Sound Open Source Supply Chain Management Strategy,” Jim Mercer, June 2022
How should organizations meet these challenges?

Given these statistics and observations, how can organizations have the confidence that open source projects are adhering to the enterprise standards they expect?

How can decision makers tell the difference between a project maintained by someone who is being paid by an employer for their open source maintenance work versus an independent solo maintainer completing their work on nights and weekends?

And should we, as enterprise users, temper our expectations regarding enterprise standards for projects backed by underpaid or unpaid maintainers?
Continued impact of open source software supply chain attacks
CONTINUED IMPACT OF OPEN SOURCE SOFTWARE SUPPLY CHAIN ATTACKS

‘The Internet Is on Fire’
A vulnerability in the Log4j logging framework has security teams scrambling to put it in a fix.

The industry has seen a barrage of supply chain attacks over the last few years. Log4Shell is the latest example and was a perfect storm; an encapsulation of both these security and maintenance challenges and supply chain resilience challenges.
Imagine what it was like to be a volunteer Log4j maintainer last December...

Log4j maintainers have worked on this project for over 20 years, with minimal compensation for their efforts. When the zero-day vulnerability was found in December 2021, those unpaid maintainers were forced to work nights and weekends trying to find a way to mitigate the issue.
Not only was Log4Shell incredibly problematic, it was also costly to remediate.

According to the latest Cyber Safety Review Board (CSRB) report:

“One federal cabinet department reported dedicating 33,000 hours to Log4j vulnerability response to protect the department’s own networks. These costs, often sustained over many weeks and months, delayed other mission-critical work, including the response to other vulnerabilities.”

---

**CABINET DEPARTMENT LOG4SHELL REMEDIATION COSTS**

<table>
<thead>
<tr>
<th>Hours lost to Log4Shell remediation</th>
<th>33,000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average hourly pay for U.S. government software engineer I</td>
<td>$124/hr</td>
</tr>
<tr>
<td>Total cost of Log4Shell remediation</td>
<td>$4M</td>
</tr>
</tbody>
</table>

**ESTIMATED TOTAL U.S. GOVERNMENT LOG4SHELL REMEDIATION COSTS**

<table>
<thead>
<tr>
<th>Number of federal cabinet departments</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td>Estimated U.S. government cost of Log4Shell remediation</td>
<td>$61M</td>
</tr>
</tbody>
</table>
Government response to open source security issues

Governments around the world are now making software security an urgent priority, driving new obligations for organizations which must now vouch for the security and integrity of open source used in their applications.

In 2021, the White House released an Executive Order on “Improving the Nation’s Cybersecurity,” stating that organizations need to, if they wish to conduct business in partnership with the government, attest to the integrity of the software that they are selling and provide the government with a list of the software components in their applications—including the open source they’re using.
CONTINUED IMPACT OF OPEN SOURCE SOFTWARE SUPPLY CHAIN ATTACKS

In early 2022, the Federal Trade Commission warned companies that it would, “use its full legal authority to pursue companies that fail to take reasonable steps to protect consumer data from exposure as a result of Log4j, or similar known vulnerabilities in the future.” As an example of their clear intentions, they cited the $700 million fine levied against Equifax for their failure in fixing a known vulnerability in Apache Struts.

Furthermore, in July of 2022, the U.S. Cyber Safety Review Board (CSRB) released a report on the Log4Shell vulnerability. The CSRB report not only reflected on the Log4Shell incident, but it presented direct recommendations on increased investments in open source security, recommended exploring “more sustainable models” for open source software security at scale, and called out the need for innovation in incentive structures for open source creators.
A call for improved security and maintenance standards

There is a growing movement to improve the overall resilience of the open source software supply chain in light of Log4Shell and other vulnerabilities and attacks. Several initiatives have already been rolled out:

- Open Software Security Foundation (OpenSSF) Best Practices Badge Program
- Center for Internet Security (CIS) Software Supply Chain Security Guide
- National Institute of Standards and Technology (NIST) Secure Software Development Framework
- OpenSSF Security Scorecards
- Supply chain Levels for Software Artifacts framework
- NIST Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
- Cloud Native Computing Foundation (CNCF) Software Supply Chain Best Practices
- Open Web Application Security Project (OWASP) Software Component Verification Standard

The core of the effort across all of these initiatives is documenting a set of ideal enterprise policies and standards that open source components should maintain to ensure good security outcomes.
As these new security standards begin to take hold, one key issue is emerging: who is going to do the work?

Because many open source maintainers are volunteers, expecting them to do more work to ensure their components meet these new standards is not a given.

The CSRB also highlighted this concern in their latest report, stating:

“[Log4Shell] also called attention to security risks unique to the thinly-resourced, volunteer-based open source community. This community is not adequately resourced to ensure that code is developed pursuant to industry-recognized secure coding practices and audited by experts.”

Or 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.”

How should organizations address these open source-related challenges?
Defense in depth: A multi-layered approach to application health and security for the open source software supply chain

At Tidelift, we recommend that organizations take a multi-layered approach to maximizing application health and security.

Many organizations are already addressing what we would refer to as reactive strategies, that give them the capabilities to identify and resolve known vulnerabilities and issues using tools such as application testing, container security, and software composition analysis. At the same time, organizations need to start thinking about proactive strategies that lead to improvements in how organizations manage open source usage internally and improve the overall resilience of the open source software supply chain.
How Tidelift can help

Tidelift is engineered to deliver these proactive strategies through a software and people based approach to managing open source.

Tidelift makes it easy to define open source standards and policies, and to create and maintain catalogs of pre-vetted and approved open source components. At the same time, Tidelift partners directly with open source maintainers, the very people who can do the work to align their projects with the industry standards described above and pays them to ensure their components meet enterprise standards now and into the future.
The Tidelift Subscription

A proactive approach to improving the health, security, and resilience of your organization’s open source software supply chain.

Software-powered

A PROACTIVE APPROACH TO MANAGING OPEN SOURCE

Tidelift provides the tools, data, and strategies that help organizations assess risk and improve the health, security, and resilience of the open source used in their applications.

• Define open source standards and policies
• Create and maintain catalogs of pre-vetted and approved open source components
• Help developers self serve and keep moving fast

People-powered

BACKED BY TIDELIFT AND OUR MAINTAINER PARTNERS

Tidelift partners directly with maintainers and pays them to ensure the open source software organizations rely on meets enterprise standards now and into the future.

• Reduce need for developers to evaluate open source components on their own
• Shorten the time to identify and remediate issues with resolution recommendations from Tidelift and maintainer partners
The key benefits of the Tidelift Subscription
KEY BENEFITS OF THE TIDELIFT SUBSCRIPTION

- Improve VISIBILITY
- Improve DECISION-MAKING
- Improve GOVERNANCE
- Improve RESILIENCE
KEY BENEFITS OF THE TIDELIFT SUBSCRIPTION

Improve visibility

Improving your organization’s open source software supply chain resilience begins with clear visibility into all of the open source components being used by your development teams.

- Dynamic SBOMs generated after every build
- Visibility into transitive dependencies for JavaScript, Java, and .NET
- Easily search for open source components of interest and understand usage
- Identify open source components that do not align with organizational standards and policies
KEY BENEFITS OF THE TIDELIFT SUBSCRIPTION

Improve decision-making

Organizations want to, but lack the ability to, make informed, data-driven decisions about which open source components and versions their developers should use.

- Human-researched metadata to drive informed decision-making
- Maintainer-verified CVE and license data
- Recommendations to improve application health
- Centralized decision engine to drive consistent development practices
KEY BENEFITS OF THE TIDELIFT SUBSCRIPTION

Improve governance

Cross-functional stakeholder alignment is an important aspect to effectively managing open source usage across an organization. In our 2022 open source supply chain security report, only 15% of organizations reported being “extremely confident” in their open source management practices, while 62% are “somewhat confident” and 22% are “not very” or “not at all” confident.

- Inclusive approach to defining open source policies and standards
- Proactively evaluate and approve open source components for developers to use
- Help developers self-serve from approved components and avoid rework
KEY BENEFITS OF THE TIDELIFT SUBSCRIPTION

Improve resilience

Open source security breaches can be costly to remediate, costing organizations both time and money. Tidelift helps development teams reduce both downtime and rework by ensuring they are building applications using pre-verified, approved open source components.

- Validate that components meet enterprise standards—with data and recommendations from Tidelift and maintainer partners
- Enable informed decision-making to resolve issues and improve application health
- Conduct necessary due diligence with research and validated metadata from Tidelift
Maintainer-validated standards

We continuously analyze and aggregate industry open source software standards and work directly with maintainers to identify and validate the important security, maintenance, and licensing standards that will produce meaningful positive health and security outcomes. Most importantly, implementing these standards has led to measurable improvements in the health of many open source packages.

- Annotating licenses
- Remediating vulnerable code artifacts
- Documenting security policies
- Properly tracking and communicating package dependencies (including bill of materials)
- Tracking and updating package dependencies
- Updating packages regularly
- Implementing two-factor authentication

TIDELIFT’S PARTNERED MAINTAINERS HAVE BEEN ABLE TO SIGNIFICANTLY IMPROVE THEIR OPENSSF SECURITY SCORECARD SCORES, EXAMPLES INCLUDE:

- urllib3 score improved 34%
- jackson-core score improved 42%
- byte-buddy score improved 39%
Why now?
The bottom line

The security and maintenance challenges that come with using open source are increasing rapidly and government requirements are becoming more complex.

The rising number of software supply chain attacks and the crisis of volunteer maintainers are increasing open source-related risk.

Now is the time for organizations to implement a proactive open source management strategy that improves application health and security and strengthens software supply chain resilience.
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