ROI CASE STORY

The value of a proactive approach to open source application security

Large enterprise customers have found a new way to proactively improve software security risk and strengthen the resilience of the open source powering their applications. This is the story of one such customer, who worked with Tidelift and its maintainer partners to save time and money.

This work drastically reduced the risk present throughout the open source dependency lifecycle — without the customer having to add new engineering staff to address the gaps. Here is their story.

Over the past two years, this customer has been focused on ways to take full advantage of the innovative potential of open source by reducing the time and money spent managing each stage of the dependency lifecycle.

Like many organizations that need to remain competitive, while handling a large volume of sensitive customer data, this customer **required** open source software. They needed a consistent operation for dependency lifecycle management between disparate internal and external contract development teams, and needed to show that they had a strategy in place that was reducing vulnerabilities in production.

Realizing that scanning software to discover and fix vulnerabilities was not getting their teams to the goal quickly enough, they prioritized a strategy to proactively prevent bad packages from entering production in the first place, while cleaning up the risk that they were already carrying.

Making decisions on which packages to use

One of the most significant challenges this organization faced was making good, consistent decisions about which packages and versions to bring into their applications in the first place. The time consuming, continuous, and error-prone process for getting information about the condition of open source packages in order to make good decisions was eating up development cycles and increasing risk.

The organization often faced rework and vulnerability remediation caused by needing to replace insecure, undermaintained, or deprecated packages. In a few situations, the organization has been harmed by a choice to use an open source package that could have been better vetted upfront.

In its first two years working with Tidelift, the organization was able to avoid over 50,000 bad releases (that had been formally deprecated, abandoned, or were otherwise unfit for enterprise use) by using data and analysis provided by Tidelift and its maintainer partners.

15,000
packages requiring analysis

1 hour
time required to analyze each package by developer at $110 per hour

$1,650,000
value of manual evaluation time saved over a two year period

THE TIDELIFT MAINTAINER ADVANTAGE

The customer featured in this story was able to benefit directly from Tidelift's unique relationship with open source maintainers. Tidelift is the only company that partners with the maintainers behind thousands of the most relied upon open source packages and pays them to:

1. Implement specific secure software development practices and validate the practices they follow so organizations can have the same confidence in the security of their open source that they have in their own code.
2. Promise to continue these practices into the future so that organizations can confidently make long term investments in the packages they use.

Previously, this customer was spending over an hour to analyze each package in order to arrive at a decision on whether to use it. The scale of this on a package basis alone was overwhelming, and the analysis needed to happen on a per-release basis to accurately assess risk. The customer realized that there was a better way to centralize and automate this analysis and decision making at scale. Over two years they needed to make decisions on almost 15,000 packages alone. This means that, at a cost of $110 per developer hour, the organization was able to save $1,650,000 in manual evaluation time over a two year period.

300

vulnerabilites fixed by Tidelift maintainer partners

3000

points of risk eliminated in applications running in production

Fixing vulnerabilities in critical dependencies

Part of this customer's challenge with reducing the vulnerabilities in production was that there were many cases where a fixed release was simply unavailable. Making the choice of whether to fork the package internally and fix it themselves or replace it with something else was also eating up developers' time. The customer needed more assurances on what packages would have a maintainer available to receive security research and issue fixes to address reported risk. Ideally, the customer was seeking a model that guaranteed security fixes and trust that their most critical dependencies would be maintained using industry best practices for secure software development.

This customer was able to benefit from Tidelift's contractual relationships with open source maintainers and realized an overall reduction in security fire drills, while getting valuable data that helped their teams prioritize and take action on risk.

Over this same two year period, the customer was able to benefit from almost 300 vulnerabilities that were fixed in accordance with Tidelift's maintainer contract. These vulnerabilities eliminated over 3000 points of risk in applications running in production.

EXAMPLE: JACKSON-DATABIND

Tatu Saloranta maintains jackson-databind and is a Tidelift maintainer partner. jackson-databind is also heavily used by many of Tidelift's customers. As a Tidelift partnered maintainer, Tatu had already implemented many required secure software development practices. This made the package more reliable for customers to use. However, jackson-databind was still being impacted by a large number of remote code execution (RCE) vulnerabilities, and this was a significant concern for many customers.

In light of this, and thanks to the money being paid to Tatu by Tidelift, he was able to devote time and resources to completely re-architecting jackson-databind and to eliminate the RCE vulnerability entirely.

Prioritizing which vulnerabilities to remediate

This customer had a pre-existing SCA solution in place, and it was valuable for finding known vulnerabilities in its open source dependencies. In cases where fixes were available, and the customer was directly using a dependency, teams could simply apply the fix. Prioritization continued to be a challenge at this scale, as this customer did not have the developer time available to apply the many fixes needed or easily prioritize which fixes were most urgent to apply first.

The customer's security team was also struggling to convince developers to prioritize the work after valuable time had been wasted on remediating SCA-reported issues that really weren't an actual risk. Needing a better way to prioritize work, the customer was looking for complementary data that could document which vulnerabilities were creating real risk for the business, as well as how to remediate them.

This customer was able to use information from Tidelift and its partnered maintainers to quickly prioritize which vulnerabilities to work on first. As an example, in one recent month, the customer's prioritized action report showed them the open CVEs on all of the packages they had in use. Using Tidelift data, the customer was able to see that 1000 of those CVEs were reported by maintainers as false positives, having a low likelihood of customer impact, or had a documented workaround already available.

Conversely, 60 of the CVEs were identified by maintainers as highly likely to have an impact (with 22 of these offering a workaround as well). Using this data, the customer was able to quickly prioritize the CVEs most likely to impact them and de-prioritize or document the mitigations for CVEs that would not impact them.

Replacing insecure dependencies and avoiding costly rework

This customer has also analyzed the amount of time required to replace packages that were abandoned, undermaintained, or otherwise insecure after they had already been included in production applications.

This was particularly painful when a move to production was delayed because a CVE was found late in development through a scanning tool. The customer estimated the average time required to replace an insecure package found late in the game versus those identified proactively at 3 months per instance!

Not only was this valuable development time that could otherwise be used to continue new application development, but these delays would also slow progress toward the organization hitting its business goals.

It's hard to know how many hours were saved because of rework that did not happen, but the customer does report that the number of situations where open source packages have needed to be replaced has declined.

Bottom line

Over the past two years, this organization has been able to reduce risk and improve business continuity by proactively improving the resilience of the open source powering their applications. They were able to achieve positive results at each stage of the open source dependency lifecycle in partnership with Tidelift.

They could make better decisions about packages up front, and gained confidence in their open source dependencies because of the contractual relationships Tidelift has in place with its maintainer partners. They were able to better prioritize which vulnerabilities to remediate first based on direct insights from Tidelift's maintainer partners, and they were able to avoid many costly rip and replace moments because problematic open source dependencies were avoided in the first place.

The directly quantifiable value of the benefits this organization received from this effort to proactively improve open source security in partnership with Tidelift easily surpassed $1.5 million over two years, and the harder to quantify benefits related to reducing risk and avoiding disruptions and rework make the actual realized value much higher.