Leading healthcare organization reduces open source risk and streamlines management costs with Tidelift

In a heavily regulated industry with growing emphasis on data security, one leading healthcare organization chose to invest in elevating the patient experience by creating an innovative patient portal that seamlessly leads people from initial intake through billing and post-care engagement.

The organization opted for an in-house software development approach, leveraging open source software extensively to speed up their development process and have the patient portal completed more quickly while also ensuring it was equipped with cutting-edge functionality. With open source playing a critical role in their application development, and recognizing the critical need to protect patient health records data with utmost care, the organization set a strategic objective to effectively manage the health and security of its open source software supply chain.

CHALLENGES FACING THIS ORGANIZATION:

- ☑ Lack of visibility into open source usage
- ☑ Manual tracking using Excel sheets
- ☑ No SBOM capabilities to meet industry requirements
- ☑ Preventing developers from introducing new security risks by giving them clear and actionable guidance on which packages and releases to use

Their existing approach to managing open source relied heavily on spreadsheets and vulnerability scanners. The spreadsheet was made up of self-reported and manually entered data, tracking only a small percentage of the top level open source software in use within the organization. The project leaders weren't able to map open source software usage to specific applications, and they had no visibility into the open source libraries in use beyond the rows listed in the spreadsheet. They had no software bills of materials (SBOMs), and technical debt kept piling up.

When their scanning tool noted a vulnerability in a library used in one of their applications, a JIRA ticket was created for every instance of the vulnerability. This meant when the Log4Shell vulnerability emerged, over a thousand JIRA tickets were created. And when vulnerabilities like these were found, the tool they were using often recommended downgrading to an earlier version of the packages in use...which just put them farther behind in the release schedule.

While the benefits of using open source software were plentiful, the challenges of managing open source usage across the organization while also keeping the business applications that stored sensitive patient data secure was keeping IT and business leaders up at night.

This was when business leaders tasked the enterprise architecture, security, and software engineering teams to come together to build a plan to address these challenges and allow the organization to take full advantage of the innovative power of open source while keeping the organization safe and in compliance.

Shifting left by partnering with upstream maintainers

Having undertaken a thorough market analysis, the teams responsible recognized the need for additional capabilities beyond what their scanning tool could provide.

Enter Tidelift, which was able to address many of their core challenges—providing centralized visibility into open source usage, including indirect dependencies, mapping which open source packages are being used by specific applications, generating automated and dynamic SBOMs each time a developer submitted a new pull request, and eliminating the need for manual tracking. Having this functionality was important for complying with regulatory requirements and also for taking timely action in the event of security issues that could jeopardize sensitive patient records.

What stood out as a differentiator with Tidelift was the ability to define standards around their open source usage, such as acceptable licenses, security practices, and version guidance. These standards were leveraged to build out a catalog of vetted and approved open source packages that developers can use to build applications.

Most importantly, Tidelift's unique and proactive approach of working upstream with open source maintainers was identified as a significant value add. This organization was able to benefit from recommendations coming directly from the maintainers about vulnerability remediation, flagging false positive vulnerabilities, and suggestions for alternative packages when available.

In addition, the organization valued that the maintainers of many of its most important open source dependencies had contractual relationships with Tidelift, where Tidelift paid them to ensure their projects follow industry-standard secure software development practices. This gave the organization even more confidence that these projects were not only being maintained to enterprise standards today, but that the maintainers would stay committed to keeping them updated into the future. This was particularly important because once the patient portal was built, many of the open source components it was developed with might be relied on for years or even decades as critical underlying infrastructure.

All of these capabilities together helped the organization shift left and in their estimation Tidelift saved them several million dollars through streamlining workflows and research costs while also reducing open source software related risk across various IT departments.

Open source management and alignment across the organization

How were these savings realized? The first quick win was the ability to create an inventory of all the open source in use by generating dynamic SBOMs every time a new pull request was submitted, helping them identify potential risk early in the development cycle. This connected open source package usage directly to the application that was using the package. It also helped the organization gain a full picture of which open source libraries it depends on, and how these packages align with the organization's standards.

If a vulnerability generates a thousand tickets, they can apply one set of recommendations, often coming directly from the open source maintainer themselves, to all those tickets. This guidance is easily digestible, too, because many of the developers working on applications are contractors and need actionable steps.

Now, instead of manually tracking packages into a spreadsheet, they have complete visibility across the entire organization. By adding Tidelift into their CI/CD pipeline, they have shifted left, providing their teams with a set of vetted packages, to help prevent net new risk; reduced technical debt; and begun the necessary task of managing their open source software supply chain more effectively.

OUTCOMES

☑ Centralized visibility into all open source software across the organization
☑ Dynamic SBOMs generated at each pull request submitted
☑ Shifting left with guidance to developers on which open source packages to use
☑ Going beyond simply addressing vulnerabilities and minimizing open source risk leading to several millions of dollars worth of savings

Unexpected benefits: making proactive decisions to reduce open source software related risks

Reacting to late-stage risk alone is no longer enough to secure your organization's software. Open source software supply chain threats are much broader than what CVEs tell us—and managing all of this at scale is overwhelming. The path out of late development stage fire drills is using data to drive action, earlier.

Tidelift combines its network of partnered open source maintainers with an in-house data team, resulting in an expansive set of open source software intelligence that is human-researched and maintainer-verified. With Tidelift's human researched and maintainer verified data feeding into their in-house risk scoring tools, the organization was able to answer questions such as:

☑ Is the project deprecated, abandoned or is it actively maintained and receiving fixes?
☑ Who are the maintainers behind the project?
☑ Does the project have basic security practices such as multi-factor authentication?
☑ Does the project have a history of responding to security and other issues?
☑ Who has publishing rights on upstream package managers?
☑ and more

These insights have helped both the security and software engineering teams think beyond just vulnerability remediation. There is now a growing emphasis across this organization on evaluating open source packages in a way that minimizes the likelihood of being impacted by issues in the first place.