

Case Study: Palamida on Palamida

Impact Highlights:

- Discovery of open source project version with known flaw that would have impacted performance and usability for customers
- Detection of embedded open source files inside of other open source projects and under different licenses saved company from legal exposure due to license violation
- Documentation of open source projects under dual license (commercial and open source) in order to ensure compliance to policy requiring use of commercial license

“We walk our talk at Palamida, running the best application security for open source available against our most important corporate asset – the software we sell to our customers: Palamida Enterprise Edition.”

Bennett Barouch,
Vice President of Engineering

About Palamida

Palamida is a globally distributed Independent Software Vendor (ISV) with corporate headquarters located in San Francisco, California. Palamida’s mission is to help organizations secure their most important asset – their custom built software applications – by offering solutions for application security for open source.

Palamida’s Challenge

Palamida sells to a range of companies, from start-ups to Fortune 50 organizations – all with proprietary information that must be protected and who require the utmost in integrity from their solutions provider. Because we distribute our proprietary software, and our product is our primary source of revenue, our livelihood depends upon delivering the best possible solutions. Any security or intellectual property issues would pose serious problems for our business.

Palamida Benefits from Palamida

Over the years, we have benefited from using our own solution in numerous ways, from the identification of software flaws in older open source software, to uncovering security vulnerabilities, to ensuring intellectual property protection.

One example that impacted an earlier version of our product concerned the use of Apache Derby, an open source software project that is a part of our technology platform. Derby is a powerful Java relational database that can be embedded in applications to process online transactions. During an alpha release of Palamida Enterprise Edition, we discovered that we were using an outdated version of Derby that has a known memory leak. This specific flaw is of no consequence in many applications, but could have been a major problem in the way we were implementing Derby, due to our very large data set. If we had not been alerted to the fact that we were using this version, the leak could have led to a complete failure of our software at customer sites.

Because Derby is an open source project, we were able to review the source code, validate the identified bug, and create a temporary fix. Like almost every open source vulnerability or flaw, the bug had already been identified and fixed in a later version. But we were able to successfully create a fix for the version we were using at the time. We contributed our fix to the Derby community, where hopefully it will be useful to another user in our situation.



In another instance, we were able to verify that we were using Click Framework, a web application framework for Java, which is licensed under Apache 2.0. Using our automated request system, our engineering team had previously received approval for the use of Click and the Apache 2.0 license, but our detection engine scanned Click and detected files embedded inside the project that were licensed differently. One set was three Java files that enable easy charting and graphing capability, licensed under the General Public License (GPL). That license is in conflict with our business model. While we are using Click, we do not require the graphing capability so we were able to remediate the issue by removing the files to ensure that we were not violating the terms of the license.

Finally, during a regularly scheduled code scan we found early in one development cycle that we were using another project, DHTML Carpe™ Slide that is dual licensed under the GPL and a commercial license. Palamida is a commercial user and in order to ensure we were compliant with appropriate license terms, we made arrangements directly with the vendor to adopt the commercial license.

How Palamida Uses Palamida

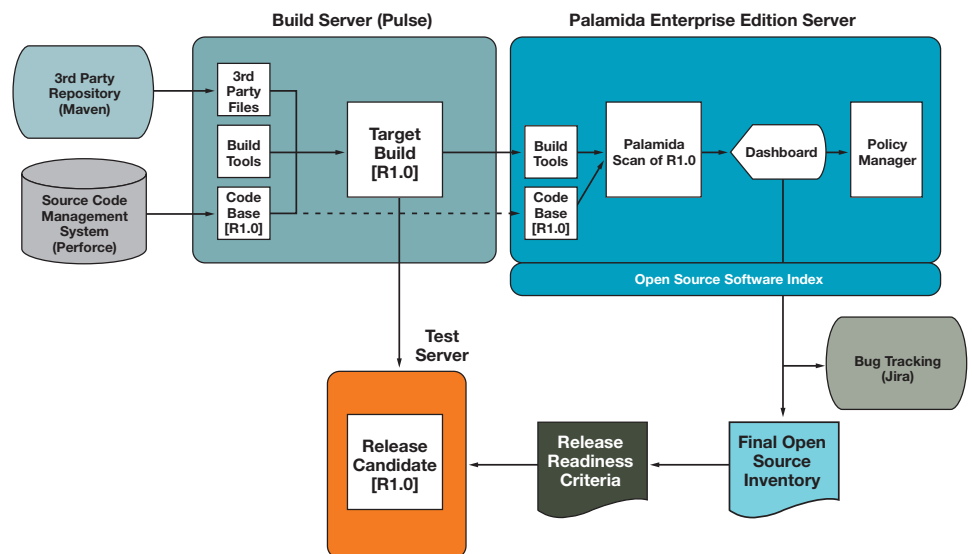
As a response to customer demands for diligence, the ISV engaged Palamida to conduct a comprehensive audit of all mission critical applications – analyzing and categorizing all open source and third party components in use. Palamida provided a complete inventory on the code inventory, as well as a prioritized list of all known open source vulnerabilities found within the code base. Palamida’s team identified security risks down to the exact line of code in which they resided, allowing the ISV to remediate outstanding issues with confidence.

The Palamida Impact

We use our own Palamida Enterprise Edition as part of our software development process and ongoing application lifecycle management. Palamida has a globally distributed development organization, and we use both in-house development resources as well as outsourced engineering teams.

We use key modules of our Enterprise Edition in the following way:

Vulnerability and IP Detection Engines: We run both scheduled and ad-hoc scans on our code base by integrating the Enterprise Edition with our build system Maven 1.0. Using our open API, we have integrated Enterprise Edition into Maven, which means that when Maven begins compiling a build, it triggers a code scan by the Enterprise Edition on the release candidate of our own product.



Palamida on Palamida Scan Overview

Vulnerability and IP Analyzers: As with any independent software vendor, Palamida has aggressive product release schedules, so ensuring that we can rely on all the available analyzers in the Enterprise Edition greatly reduces the time and headcount that would normally be focused on tedious manual analysis in reviewing false positives.

Dashboard: There is a cross-functional team involved in reviewing issues and alerts that come from our scans – engineering, product management, executive staff and legal. All of our engineers receive alerts containing questions related to code they wrote. Our product manager reviews the inventory of open source projects we are using at different parts of the development cycle. Executive staff at Palamida receives alerts when projects, versions and licenses appear that are outside of our security and IP policies. When issues appear that need to be reviewed by our outside legal staff, we generate a report that can be sent for review. In addition, remediation issues that impact our code base are entered into Jira Enterprise Edition v3.7.3, our bug tracking system. A final inventory of open source components, versions and descriptions is archived on the server and accessible via the Dashboard for ongoing monitoring.

Policy Manager: Over the years, our security and IP policies have continued to evolve. An open source project version that was on our whitelist a year ago is now on our blacklist because the community identified a vulnerability in the project that impacts us. We use open source projects which are dual licensed – so the commercial license is on our whitelist, while its open source counterpart is on our blacklist.

For a full inventory of open source projects, versions, and licenses that Palamida uses in our software products, email info@palamida.com.

Palamida

Palamida has demanding customers and financial backers who require the highest quality product with exceptional usability. By running Palamida Enterprise Edition, on our own products we have been able to live up to these expectations and have been able to avoid both security and IP issues that would have been costly and unnecessary.

By using our own solution we are able to confidently ensure the security of the software we deliver to our customers. In turn, our clients can be certain that our solution protects them from potential vulnerabilities and IP infringement within their own custom applications. It is a win-win solution for all.



PALAMIDA[™]

Application Security for Open Source Software

215 Second Street
1st Floor
San Francisco, CA 94105
P: 415.777.9400
F: 415.777.5800

www.palamida.com