

Case Study: Financial Services ISV

Impact Highlights:

- Palamida's code base audit took 2 days – saving the company the equivalent of one-man month's worth of work
- In depth reporting closed the gap between engineering and IT teams – enabling both to track new and emergent vulnerabilities as soon as they are recognized
- Full bill of materials was included with product distribution to all clients to eliminate FUD during purchasing and implementation phases

“Palamida found 40% more open source and third party components than we had previously documented – some that had multiple vulnerabilities associated with the versions we were using.”

About the Company

Leading provider of technology software products to retail financial services organizations. In business for over five years, this ISV counts among its customers some of the best-known financial services firms on Wall Street.

Business Challenge

Today's organizations are held to strong customer expectations and increasingly strict compliance standards regarding the security and integrity of both their business practices and their products. As the overall awareness of risk has increased, so has the inclusion of application security as a core component of corporate due diligence and compliance processes. Customers would often request a full disclosure of all application components, as well as a risk assessment on security vulnerabilities as part of the purchasing process. Because the ISV's products support key online banking applications at customer sites, security intelligence is an integral part of both the sales and implementation processes of their software.

Benefits

The ISV had an established process and policy for implementing open source and other third party code into their product line, but verification of compliance to policy was done through manual code review. Palamida's preliminary audit of the code base found nearly 40% more open source and third party components than originally declared by the ISV. Additionally, the undocumented code contained vulnerabilities related to outdated open source projects residing in mission critical portions of their application. The presence of undocumented and vulnerable code exposed the ISV to legal and security risks that could have had repercussions for their business and that of their customers.

Having a complete inventory of all open source and third party components enables the ISV to provide an up-to-date information to their customers, and ensures that they are in compliance with existing mandates surrounding due diligence. The audit process also laid the groundwork for the ISV to update and change existing software development practices as well as usage and procedure policies.



How the ISV Used 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

Palamida provided the Company with a comprehensive inventory for all open source and third party components and versions within their code base – with detailed security and intellectual property intelligence. This intelligence included multiple associated vulnerabilities due to outdated use of open source versions, license, and copyright information. In addition, the audit report supplied detailed evidence of open source use and its exact location – down the file level – to assist in remediation efforts. Due to the nature of their business, the ISV is committed to both security and efficiency surrounding the development of their product. Using Palamida's audit services delivered the depth and insight necessary for the ISV to rectify any potential security issues, if found, before deployment at customer sites.



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