PALAMIDA™
Application Security for Open Source Software

PRODUCT BRIEF

Palamida: Enterprise Edition Integration with IBM Rational ClearCase

Extended Protection for Application Security

Every organization developing software and Web applications today is faced with the challenge of delivering higher quality, more capable products and services within tighter schedules, and with fewer resources. Leveraging open source software is the key to meeting this challenge. Without a well thought-out strategy for the use of open source, no software development organization can effectively compete. A typical organization treats the use of open source informally - in other words, without the policy, training, and process needed in order to identify what open source components are used in a development project and whether they are free from vulnerabilities. This informal process represents a critical new gap in an organization's application security strategy.

Gartner, Inc. advises organizations to close this gap using a new set of tools and services for software composition analysis – identifying open source in use, their location, and associated vulnerabilities in order to ensure the security of all applications. Palamida's software composition analysis system, integrated with IBM's® Rational® ClearCase® extends application security further into the development cycle.

Think hidden open source with vulnerabilities is not a problem? Think again.

Applications developed within the last five years typically contain 50% or more open source and other third-party components. While open source provides many benefits to the software community, approximately 60% of its use goes undisclosed and is not formally identified and tracked as part of a development project. This fact poses significant threat to the security of custom-built Web and software applications, since it is impossible for organizations to secure what they do not know they have.

Use of open source components is good – it has lowered the cost of development and enabled companies to deploy new applications sooner. Palamida has found, however, that 7 out of 10 open source components have security vulnerabilities categorized as medium or high in severity. Most open source communities have patches to the vulnerabilties within hours or days. But since only 1 out of every 10 open source applications has commercial support, it forces end user organizations to manage those updates themselves.

70% of applications scanned by Palamida have open source with vulnerabilities ranked as either high or medium in severity.

It is imperative for organizations to identify the vulnerabilities within their applications, and critical for them to assess the impact of those issues to determine the best course for remediation. Palamida and IBM customers can now benefit from an integrated application security solution for their open source software use.

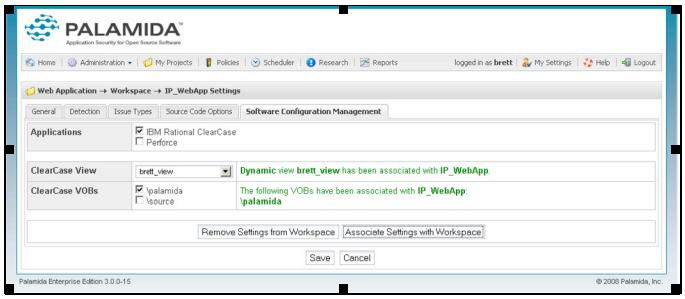
The power of integration

Integration between Palamida Enterprise Edition and IBM Rational ClearCase enables automated code audits, the process of inventorying the open source software in use and alerting on security vulnerability issues, as part of the normal application build and release cycle.

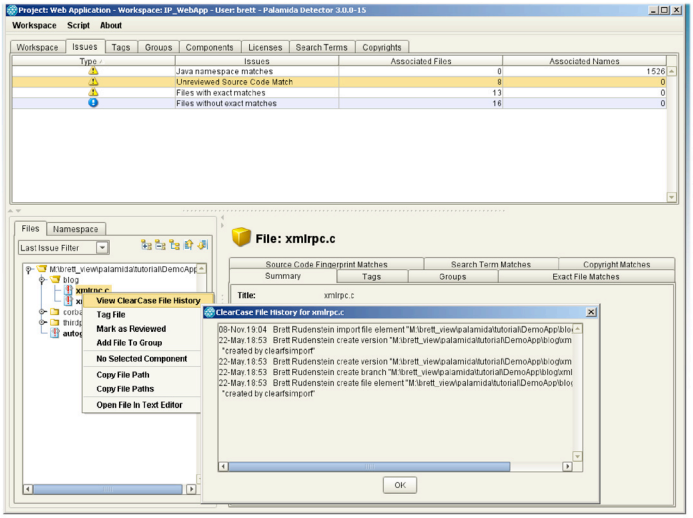
Integration with Rational ClearCase for software composition analysis at key phases of the software development process:

- Allows customers to perform automated source and binary analysis by project or portfolio, either as part of builds or within the QA process.
- Enables views to different parts of the enterprise code base in order to identify and manage one-off or scheduled scans.
- Provides dynamic flow of information between both systems enabling users to retrieve information such as comments, associated project, and other file information for faster remediation.

The integration helps ensure that security vulnerability and intellectual property issues are exposed early in the application development cycle when remediation is simpler and less costly.



IBM has been a leader in supporting and promoting open source software. An important aspect of pervasive open source use is the management and security of it within mission critical applications. The Palamida Enterprise Edition enables organizations to create an inventory of open source in use and then identifies issues of intellectual property violations and known security vulnerabilities. The software sends online vulnerability alerts as updated by the National Vulnerability Database and the Palamida R&D lab. It also enables organizations to annotate and tag all files and directories, creating a permanent record of the software composition of applications, and minimizing the security void arising from undisclosed code. The latest 6.1 terabyte Palamida data library is also included along with 29,000 open source releases with vulnerability alerts.



Protect yourself with Palamida and IBM

Integration with IBM Rational ClearCase provides mutual customers the following benefits:

- A new level of security functionality for increased return on investment in using IBM Rational tools and services.
- Complementary application security solution to IBM's existing security software such as IBM Rational AppScan, which enables static testing of source code. With the new integration, joint customers now have a solution for software composition analysis, addressing open source vulnerabilities, including those in binary form.
- A reliable framework within the development cycle for security and IP stakeholders to collaborate in the approval, analysis, and remediation of security and IP issues. Users receive alerts of violations against established policies and can archive remediation decisions.

About Palamida

Palamida provides the industry's first application security solution exclusively for open source software. The Palamida Enterprise Edition uses component-level analysis to quickly identify and track undisclosed code and associated security vulnerabilities, as well as intellectual property and compliance issues. Using Palamida, organizations can cost-effectively manage and secure mission critical Web and software applications. Customers include Avaya, Cisco Systems, EMC, Microsoft, and Sun Microsystems, among others.

For more information visit: www.palamida.com.

Contact Us

For more information on how Palamida can help your organization mitigate risk and meet application security standards and regulatory compliance, contact us at sales@palamida.com or (415) 777-9400 x123.

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

© 2009 Palamida, Inc. All rights reserved. Palamida and the Palamida logo are trademarks of Palamida, Inc. All other trademarks and registered trademarks are the property of their respective holders.