



Palamida Compliance Edition

Application Security for Open Source

Palamida Compliance Edition At A Glance

- A single system for collaboration among development, legal and security teams for license and security policy compliance
- Patented search engine algorithms yield accurate and comprehensive results for both source and binary materials
- AutoExpert™ rule-based detection learns from the results of scans to make future analysis faster and more accurate
- Innovative visualization feature makes large codebases understandable and actionable
- Automated vulnerability updates and version detection insure that new issues affecting your project are immediately flagged
- QuickReview™ simplified review feature allows stakeholders to monitor the progress of remediation
- Incremental scans minimize rework
- Branching simplifies release management

Palamida Compliance Edition is an end-to-end solution to identify open source and other third-party content contained within software projects. It enables stakeholders from development, legal and security teams to manage policy for use and take appropriate actions to secure deployed software against risks from both intellectual property infringement and security vulnerabilities.

Identify

Detection plus learning makes the system more valuable with each use

Palamida Compliance Edition uses ten individual detection techniques including source code analysis, copyright and license detection, exact file match, Java namespace analysis, among others to insure that code origin is accurately determined regardless of whether the materials available for scan are in source or binary form. In addition, AutoExpert™, a new rule-based capability allows the system to learn from analysis results and create Multi-indicator Detector (MID) Rules, a unique combination of evidence that automatically identifies the presence of a software component and records its license and vulnerability status. AutoExpert™ makes the Palamida Compliance Edition the most automated and accurate solution for software composition analysis available today.

Manage

Maintain an organization-wide view of policy and compliance

The more development teams rely on externally written code, the more they need a framework to create and manage their policies for use. Palamida Compliance Edition provides a single solution to create and maintain policies, to review the scan results, and to monitor any remediation that may be required. Together, these capabilities ensure that all decisions about what goes into a software project are aligned with the policies of the organization and fully documented.

Secure

Frequent updates keep development teams informed of security issues

The shift to open source code has made development teams more dependent on external developer communities to find and fix security and other types of issues that were previously addressed in-house. Palamida Compliance Edition delivers timely updates on new vulnerabilities within the open source components in use in development projects to.





A constantly updated library of open source material means that Palamida IP and vulnerability detection engines have both recent and legacy versions of open source material for the most comprehensive search results.

Over 250,000 projects monitored

1.5 million Releases

1.6 billion Files

2.9 billion Source Code Fingerprints

Vulnerability and IP Detection and Analysis

Software developers have over one million popular open source project versions to choose from when building custom applications – an enormous benefit in terms of cost and time savings. However most open source use remains undocumented, in other words, without a formal record of its existence within your mission-critical applications and products. The core of Palamida Compliance Edition is a special purpose search engine which uses patented Massive Multi-pattern Search algorithms and a reference library of hundreds of thousands of open source projects to scan software and identify components, partial components, and versions actually in use. Detection capabilities include analysis of binary files, source code, Java namespace information, copyright, license, user-specified terms, URLs and email addresses. Languages supported include C, C++, Java, JavaScript, Perl, Python, Action Script, VB, C#, Ruby, TCL, VHDL and Verilog. Together these techniques and language coverage insure a high probability of detection of third party code no matter what type of materials are available to scan. In particular, the ability to scan binary files and archives means that the detection engine can make accurate identification even when source code is not available – a capability that is not available using manual analysis or simple in-house tools.



ID	Name	Component	License	# Files	Priority	Review Status	Actions
25	commons-beanutils 1.7	apache-jakarta-commons-beanutils	Apache License, Version 2.0	1	4 - Low	Approved	
24	commons-codec 1.3	apache-jakarta-commons-codec 1.3	Apache License, Version 2.0	1	4 - Low	Approved	
23	commons-io 1.4	apache-jakarta-commons-io 1.4	Apache License, Version 2.0	1	4 - Low	Approved	
22	commons-lang 2.3	apache-jakarta-commons-lang 2.3	Apache License, Version 2.0	1	4 - Low	Approved	
20	cglib 2.1	cglib 2.1	Apache Software License, Version 1.1	1	4 - Low	Approved	
19	codehaus-extrem 1.1.2	codehaus-extrem 1.1.2	BSD License	1	4 - Low	Needs More Information	
17	dom4j 1.6.1	dom4j 1.6.1	BSD License	1	4 - Low	Pending Review	
14	gain-blogger	gain-blogger	GNU General Public License (GPL) Ver. 4	1	1 - Critical	Rejected	
13	hibernate 3.1.3	hibernate 3.1.3	GNU Lesser General Public License (L.G.)	1	2 - High	Approved	
11	openjdk-openjdk 2.5.1	openjdk-openjdk 2.5.1	OpenSDK License	1	2 - High	Pending Review	

The project inventory view combines component, version, license and vulnerability information in a single page, with the links to detailed information

Content Mark-up

Building an accurate inventory report is fast and accurate with Palamida's unique group capability. Groups are user-defined subsets of the files that make up the software under analysis. For example: all the files that make up the component zlib 1.2.3; all the files that contain a specific copyright; all the files that make up an internal tool; all the files that have been reviewed, etc. Analysts can tag files, perform filter operations, and create groups based on the results. In addition, groups are automatically created by the system to speed analysis work. The ability to create and retain groups moves knowledge of what makes up a codebase from the informal understanding of key team members into a structured reusable document.

AutoExpert™

The ability to learn from the analysis of scan results is a major advance in automation. Combining evidence from file path name, file contents, exact file description and Java namespace where applicable, enables the system to pinpoint components without further human analysis - greatly reducing the cost of ownership, and improving the accuracy. Palamida's AutoExpert™ includes a library of Multi-Indicator (MID) Rules, and allows users to add their own custom rules whenever necessary.

IP Analysis

Intellectual property risk centers on the potential for infringement of license obligations. Palamida Compliance Edition uses the results of component identification and license detection to provide development and legal teams with a clear and concise description of the software components in use

and their licenses. Policy information is visible throughout the system and allows users to see policy guidance and issues without changing context.

Vulnerability Analysis

An accurate report of vulnerabilities requires not only the ability to identify components, but also ability to identify versions of components, since vulnerabilities are specific to versions. Vulnerability detection in Palamida Compliance Edition uses information from the National Vulnerability Database, a service sponsored by the U.S. Department of Homeland Security, to accurately report on a wide range of security and vulnerability issues in the versions of software components used in your projects. The combination of accurate identification of vulnerable versions and their location within your code and the update service which continually delivers the latest vulnerability information insures that development teams are able to maintain a high level of application-level security with a minimum of time-consuming research.

Manage Compliance and Collaboration

Palamida Compliance Edition combines scanning with a QuickReview™ capability that enables efficient review of code audit results, and enables stakeholders from development, legal and security teams to conduct efficient reviews.

QuickReview™ is a fast, efficient way to review the often large number of code audit results. It is as simple as a spreadsheet, but is fully integrated into the system. Designed to be used in a conference room or on a conference call, it enables stakeholders to approve, reject, post comments and questions, and create checklists for remediation.



Each inventory item is summarized for review by stakeholders

Integrate With Existing Tools and Development Processes

Palamida Compliance Edition is designed with a rich set of APIs and an integrated scripting language to make it easy to include within an existing set of software development tools and processes. The included scripting language (Groovy) makes it easy to add custom reports and features accessible from within the product. Scans can be configured and initiated remotely, and the resulting scan data can be exported in a variety of formats. Preconfigured connectors are available for ClearCase™ and Perforce™.



Compliance and Collaboration Benefits

- **Single system of record for all composition history across the organization**
- **Role-based access maintains “need to know” security**
- **Flexible request workflow allows review based on request type**
- **System maintains status of remediation for identified issues**



Product Structure

Included Features	Enterprise Edition	Compliance Edition
Component Request Workflow	•	
Compliance Library	•	•
Scan Engine	•	•
IP & Vulnerability Detection	•	•
Tag-Filter-Group	•	•
AutoExpert™	•	•
Integration Framework	•	•

Recommended System

Server Hardware:	16 GB Memory 500 GB disk space
Recommended Operating Systems:	Red Hat Compliance 5 64-bit Windows Server 2008 R2 Compliance 64-bit
Supported Operating Systems:	Windows XP Pro 64-bit Windows Vista Ultimate 64-bit RedHat Compliance 4 64-bit Windows Server 2003 Compliance Edition 64-bit Windows 7 Ultimate 64-bit CentOS 5
JDK:	JDK 1.6 (update 17 or later) 32-bit for clients, 64-bit for servers
Supported Databases:	mysql Server 5.1.x Oracle 10g r2

About Palamida, Inc.

Palamida delivers application security solutions based on software composition analysis. Using our software and services, our customers identify and track open source and other externally-written software in their development projects in order to manage and secure the software they write against risks resulting from embedded software vulnerabilities and from infringement of intellectual property rights.

Contact Us

For more information, please contact Palamida at sales@palamida.com or (415) 777-9400 x 123.



PALAMIDA™
Application Security for Open Source Software

215 Second Street

2nd Floor

San Francisco, CA 94105

P: 415.777.9400

F: 415.777.5800

www.palamida.com

© 2010 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.