

Palamida Enterprise Edition 3.0

Application Security for Open Source

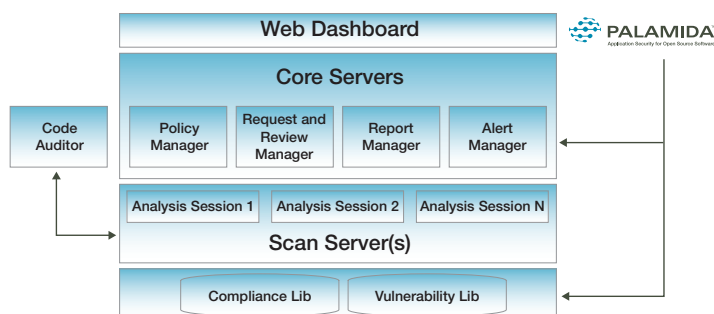
Today's software development world is complex and fast-paced. Software engineers are under increasing pressure to deliver large, high quality applications in less time, with fewer resources. As a result, the use of community-based open source software components has become one of the dominant trends in software development.

Applications developed within the last five years – whether internal or external – typically contain at least 50% open source software and other third-party components, much of which is undocumented, not formally identified and tracked as part of a software project or product.

Palamida software is the industry's first solution to address the application security problem for open source. Our software tools will analyze an entire code base, including source, text and binary files, identifying every piece of material from an Open Source project down to a few lines of code in a source file. All evidence of open source usage is highlighted so it can be documented and tracked for secure usage of the individual components in your application.

Once documented, there are no more surprises. You will know about the potential vulnerabilities in your product that arise from your open source usage. You will know about licenses and copyrights from your open source usage so there are no surprises down the road from IP infringement. You will be automatically notified about new vulnerabilities in the open source you use. You will know the implications due to license changes in newer versions of the open source you use so upgrades can be done safely.

Our software is designed to facilitate your use of open source throughout the software development lifecycle - from the first phase of application design through development, testing, and after deployment. For the first time, managers, security professionals, and lawyers have direct insight into the vulnerability and IP risks from open source use in your applications before there is a problem.



Palamida Enterprise Edition 3.0 Architecture

In today's environment, you must use Open Source to be competitive. Now, with Palamida, you can do so safely and securely, avoiding the potential liabilities from inadvertent IP infringement and vulnerabilities from un-patched code.

Palamida Enterprise Edition is a scalable solution designed to manage open source usage in projects across the enterprise. The architecture of the product is based on a multi-server, distributed architecture that can scale to meet the demands of even the largest development organizations. The key components of the system are:

- **Core Server** that delivers all of the functionality of policy, requests, reviews, reports, etc. to the entire organization
- **Web Dashboard** delivers overall status, project management capabilities, and general administrative functions such as user management
- **Policy Manager** defines the acceptable use policies for open source, allowing automated approvals (and rejections) to be set up for efficient review when manual inspection is not required
- **Request and Review Manager** facilitates developers requesting open source components for use as well as all of the review process for those requests, including the review process to tie it to the inventory from code auditor
- **Report Manager** provides complete project compliance reports as well as other specialized reports to facilitate project documentation throughout the process
- **Alert Manager** automatically generates alerts for new vulnerabilities associated with open source components in your inventory
- **Code Auditor** is a specialized tool that facilitates the review of scan and analysis results, capturing a wealth of information on the open source usage for later reporting and management
- **Scan Servers** are the scan and analysis engines that match your codebase against the Palamida libraries to exposed the open source usage in your codebase
- **Palamida Libraries** are the compressed representation of the over 6 Terabytes of open source reference material that Palamida uses when scanning your code

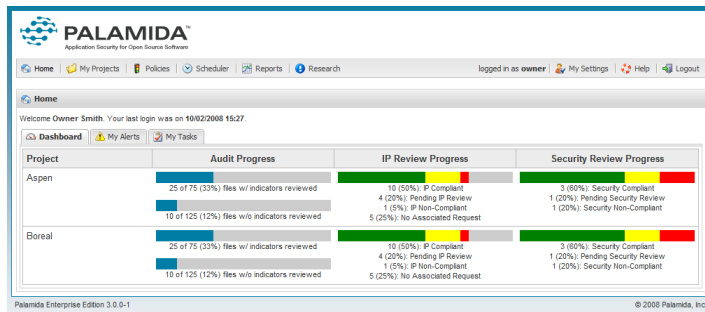
Enterprise Class Architecture

The hub of Enterprise Edition 3.0 is the **core server** that manages all of the data in the system, coordinates all activities and presents each user with the appropriate information for their role in the organization through the UI. The server is based on an open source Web Application server, providing flexible deployment options. Combined with an external SQL database for storage of project, audit, policy and other system information, the application delivers enterprise class scalability, reliability and robustness.

Monitor Projects across the Organization

The **WEB Dashboard** Enterprise Edition 3.0 provides a rich set of information that enables managers and others to quickly see the overall status of project compliance across multiple projects in the organization. From this view, it is simple to drill down on any problem area, such as a project where the reviews are not completing, and find where the bottleneck is and then take steps to correct the situation.

The dashboard is customized to each role, so another user, such as a security analyst, would see the information relevant to them, such as vulnerability review progress and any alerts for new vulnerabilities. Especially for occasional users, this greatly simplifies the application for them, making their participation in the process efficient and effective.

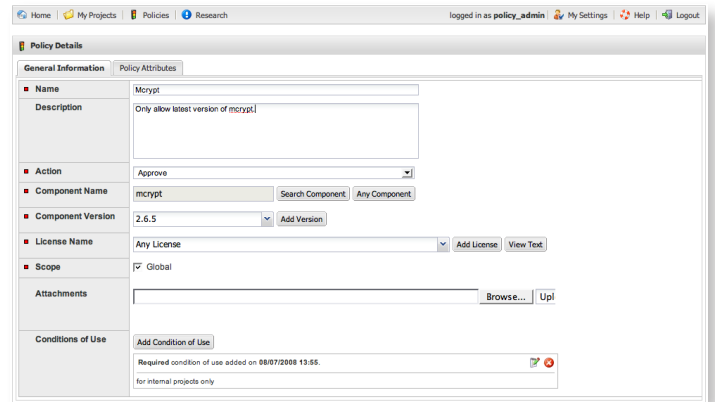


Establish Policy across the Organization

The policy manager provides a framework for defining and applying policy to open source usage throughout the organization. Policies are defined at multiple levels:

- **Global** level to define the corporate wide standards, such as no GPLv3 licenses in any shipping product
- **Group** level to augment global policies for specific organizational units that have specific needs
- **Project** level for the finest grain control at an individual project or product release

Policies can be based on a variety of criteria, including component, license, usage within project, shipping status, modification, etc. For each policy, an action is included that is applied to a request when it is submitted for review. This action selected can be manual review, automatic accept, or automatic reject, allowing for By using the automatic actions where appropriate, such as automatic accept for vaulted, corporate approved components, approval is immediately granted to developers requests', allowing them to move forward in their development efforts.



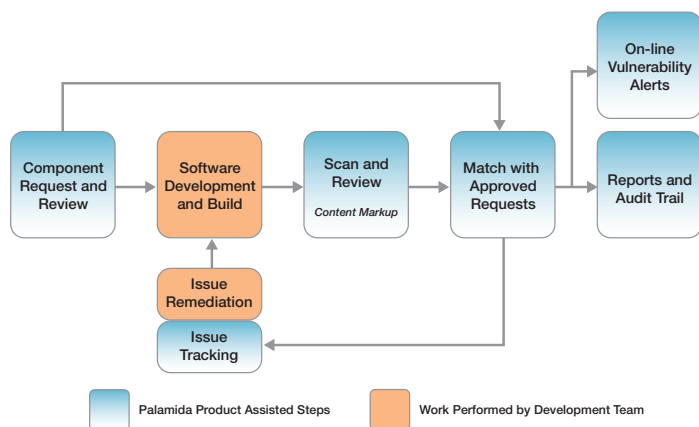
Document Intended Use

Request and Review Manager is a flexible workflow tool that manages the overall compliance process pulling together the development request and review process with the compliance and security audit process to develop a fully compliant Open Source inventory for a project. The process ideally starts during the design and early development phase of a project to help ensure the choice of open source components meets approved policy before building them in, reducing or eliminating costly remediation from non-compliant usage found late in the product development lifecycle.

The manager provides a customizable interface that guides the developer through the process of requesting a component, including information on how it is used, is it modified, what license is it under, etc., so that it can be matched against policy in the review cycle. To assist in selecting components, a research tool is provided that simplifies the developer's task of finding an appropriate component and specific version. For instance, it will show known vulnerabilities by version for the components, allowing the developer to make an informed choice and to include information regarding applicability in the expected deployment to speed the security review process. The developer can also easily review the policy for their project to identify prohibited licenses, etc., that can guide their selection as well.

Completed requests are sent through a policy review, and prompt notification is sent back to developer with the review status, rejected, accepted or submitted for manual review. In the manual case, the proper reviewers are also notified so that they can begin the review process.

The review process is defined for each project, allowing multiple steps in the process as appropriate. At any step, a review can reject, approve or *conditionally approve* the request. If conditionally approved, the developer must agree to the added conditions for final approval. This reduces the number of rejections for many issues, thus speeding the review process along.



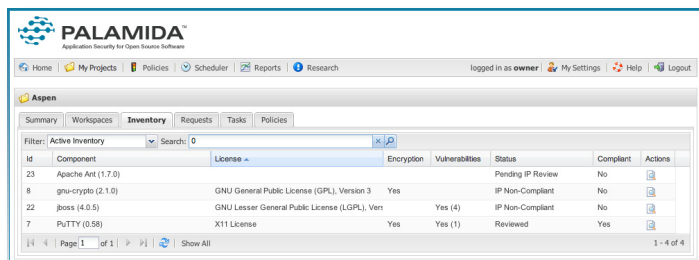
Palamida in the Software Development Process

Validate What is Really in the Code

Code Auditor presents all of the evidence from a codebase scan and enables files, groups of files, and directories to be annotated to create a permanent record of the composition of the software. It is through this tool that the code auditor acknowledges which third party and open source packages are found and any particular information that is known about them. This information is then made available to the rest of the organization as the project inventory.

The content markup provided in the code auditor is fully customizable, allowing the capture of any desired information during the code audit. Once captured, it is available now and in the future as input to decision making, including terms of use, pricing, security, export control, royalties, etc. Future decisions can be made quickly and accurately - saving time and expense

Audit Manager ties the expected components, as documented through the request and review process, with the inventory as determined by the actual code audit of the project. By associating inventory items to component requests, the auditor documents that the design matches the delivery in terms of open source usage. Any discrepancies between requests and inventory illuminate areas for further investigation to ensure the compliance of the final product.



Manage and Document the Project

Report Manager provides reporting functions for both individual projects as well as aggregate information across multiple projects. Some of the reports included are:

- Project audit report detailing all of the information gathered during the audit process
- Vulnerability report to see information specific to vulnerabilities in a project
- Unattributed source files to see any file without copyright to identify potential IP leakage
- Attribution report to show all attributions within a project

The report system is customizable, allowing the organization to alter existing reports or design new reports to meet their specific needs. This also allows reports to include custom information created through the Code Auditor.

Alert Manager coordinates and delivers external notifications to users through email. One of the key capabilities it delivers is automatic notification of new vulnerabilities against existing project inventory. Whenever the Palamida Library is updated, the system automatically matches new vulnerabilities against components in project inventory and sends an alert automatically to warn of a potential new issue.

The Heart of the System

Scan servers contain the heart of the system, the Vulnerability and IP Detection Engine. Our detection engine is based on patented Massive Multi-Pattern Searching technology, and is essentially a special-purpose search engine that is optimized to rapidly scan and match any code and content base against a very large library of known open source material. The engine is capable of scanning the widest range of software assets in the industry including source files for Java, JavaScript, C#, C/C++, Perl, Python, PHP and Visual Basic. If source code is not available, the software can detect licenses, java namespaces, binary files, copyright text, and even text files as part of its identification of open source usage.

Any automated search will typically yield a large number of matches, not all of which are indicative of results of interest. Palamida Enterprise Edition includes patented ranking and filtering software, Coderank, which analyzes the results and ranks them in terms of relevance, making reports and summaries concise and productive. In addition, because different code bases may not have the same security or IP policies applied to them, the detection engine enables organizations to fine tune the audit to accommodate a particular application, component or Web service.

Multiple scan servers can be deployed within a single instance of Palamida Enterprise Edition. This allows for additional capacity for scanning, as well as appropriate deployment for access to source code repositories. Locating the scan server near the code repository greatly improves performance and security, and in a large, geographically dispersed organization it may be advantageous to deploy multiple servers.

The Palamida Open Source Library contains 6 terabytes of open source material collected from archives around the world. The library material is compiled and compressed for delivery into two bundles, the Compliance Library focused on IP detection, and Vulnerability Reporting and Management. Together they contain information including:

- 1.1 million open source project versions
- 15 Billion source code fingerprints
- 725 million release files
- 18 million java namespaces
- Over 4,500 vulnerabilities associated with OSS versions

Reference material for the libraries are continuously collected and new library updates are made on a regular basis, including on demand updates for vulnerability information to ensure that the latest information is always available and alerts are promptly generated when new vulnerabilities are reported in the community.

About Palamida, Inc.

Palamida delivers the industry's first application security solution exclusively for Open Source Software that uses component-level analysis to quickly identify and track undocumented code and associated security vulnerabilities as well as intellectual property and compliance issues, enabling organizations to cost-effectively manage and secure mission critical applications and products.

Contact Us

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

For additional information on Palamida's other products, including Standard Edition and Compliance Edition, as well as Professional Services capabilities, visit www.palamida.com/products.



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