FLEXERA SOFTWARE®
FlexNet® Code Insight™

DATASHEET

FlexNet Code Insight

An end-to-end system for development, legal and security teams to set and manage policy for use of open source and third-party software

Benefits At A Glance:

- Multiple levels of analysis from quick assessment to detailed forensic analysis to satisfy varying business needs.
- Proven request and authorization workflow enables developers to request and receive permission before new code enters the codebase, and maintains history of the request and usage details.
- Vulnerability alerts notify development and security teams if new vulnerabilities are reported for components in use.
- Generates third-party notices files for compliance with license obligations.
- Patented scan and analysis technology yields comprehensive scan results for both source and binary materials.
- Automated detection rules make analysis faster and more accurate. Over 2.5 million rules and growing.
- Update service adds components, versions, licenses, rules and vulnerabilities weekly (sometimes daily) so that the system is always provisioned with the latest information.

FlexNet Code Insight is an end-to-end solution for managing open source and third party code in software development projects. With a growing library of 12.9 million open source components and over 2.5 million automated detection rules as well as integrated request and authorization workflow – FlexNet Code Insight is comprehensive and increasingly automated.

It allows organizations to implement a full cycle solution starting with the request to use, followed by scanning and reconciliation of actual to requested content, and finally with production of compliance documents and on-going monitoring for vulnerability and intellectual property alerts.

By gaining visibility and control of all open source software (OSS) and third party content, organizations can fully benefit from an open source development strategy while minimizing exposure to intellectual property and vulnerability risks.

Comprehensive and Accurate Scanning

FlexNet Code Insight's special purpose search engine is optimized for analysis of source and binary files using a number of detection techniques. Detection of open source materials is based on comparison of the target codebase with the contents of the Compliance Library, a large database of open source projects, which includes version and license information. By providing continuous updates of the Compliance Library with new open source releases using both automated detection and manual techniques, users get accurate and timely results, whether the requirement is a quick search for top level issues or a detailed analysis.

Automated Analysis with Autoexpert

A continuously updated and expanded set of detection rules and multiple proprietary analysis techniques make examination of scan results increasingly automated. The function of rules is to analyze scan results using known associations between scan results and open source artifacts. When a rule fires, the first operation is to create a placeholder for the presence of the open source component (a group) and add as much information as possible to the group, including component name, version, license, license text, copyright text, known vulnerabilities and any notes which further describe the component.

FlexNet Code Insight includes rules based on human analysis of the most commonly used open source projects and via automated analysis of repositories. Users can also create their own rules to automate reporting of items which are unique to their projects. Utilizing multiple proprietary analysis techniques, FlexNet Code Insight performs component-level, package-manager and binary analysis on your codebase to quickly build inventory and produce reports, including:

Source Code

Unlike a web search engine which has a single search parameter per search, the FlexNet Code Insight search scan engine breaks a source code file into many individual searches (snippets) so that the system can identify partial matches to open source. Matches from the most likely origin file and matches from other files are highlighted to ensure that the analyst has a complete picture.

Binary

A file hash (MD5) is compared against known OSS file hash values from the compliance library and matches are reported as exact matches. In addition, string, copyright, license text, and email/URL detectors are available for text that survives compilation. Releases (components + versions) containing the files with evidence (string, copyright, license text and email/URL) are displayed. MD5 hash values are also used for some types of detection rules to make component identification automatic.

Licenses

Files are scanned for “license text” in the FlexNet Code Insight database of licenses and detected licenses are displayed in a list. When an individual license match is selected, the file containing the match is then highlighted in the file tree, and can be opened for viewing.

Copyrights

Files are scanned for text that matches patterns typically used to express copyrights. After the scan, copyrights are displayed in list form. Individual copyrights can then be selected and the file containing them can be viewed.

Text Strings

Specific text is often a good indicator of third party code. For example “taken from” is an obvious signal for further investigation. One of the best practices in code analysis is to add a list of such strings during scan configuration. Once detected, the strings are displayed in list form so that the analyst can view the files.

URLs and Email Addresses

Files are scanned for text which matches patterns typically used for URL and emails. After scanning, URLs or emails can be selected and the corresponding scan results are displayed in list form. Individual URLs or emails can be selected and the file containing them can be viewed.

Java Namespace

Specialized features make analysis of Java code efficient and productive. By clicking on the namespace tab, the file tree displays compiled namespaces which is useful for finding license issues within JARs.

Advanced Audit Analysis

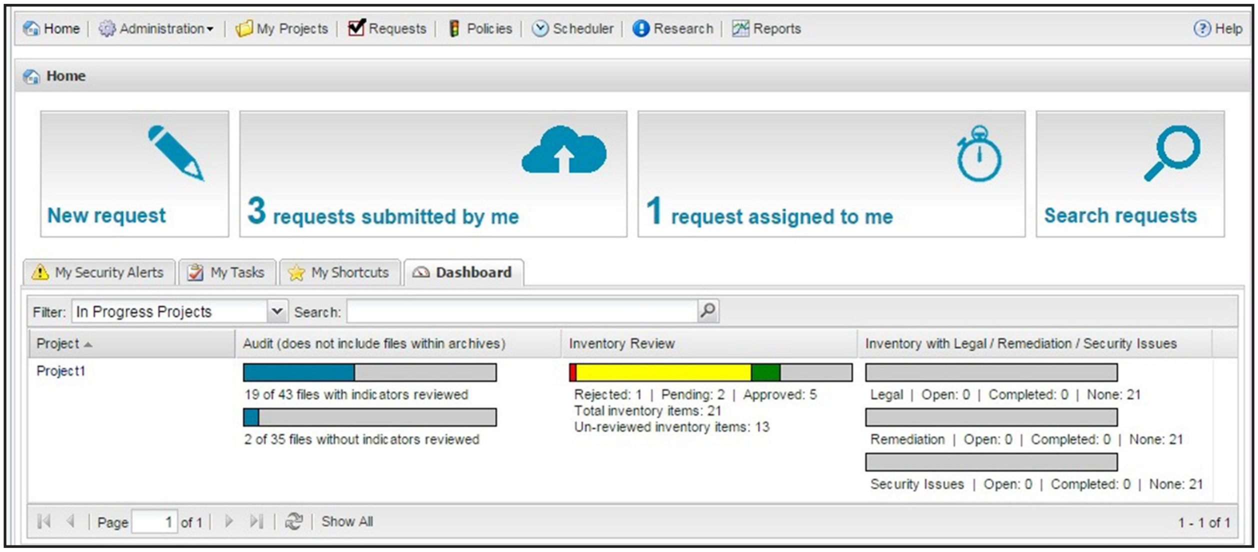
Detector Code Search: Fast, efficient ad-hoc searching across the scanned codebase—improving the auditor’s ability to detect and manage commercial third-party content, to discover references to files of unknown origin and to identify and remove false positives.

Source Code Fingerprints: Sophisticated proprietary source code fingerprint and snippet matching helps users conduct detailed and forensic level analysis. Highlights are available for matches to third-party components from multiple sources, making it easy to identify copy-paste and stolen-from code.

Custom Fingerprints: Commercial and proprietary code may be fingerprinted using the Custom Fingerprint technology for inclusion in the FlexNet Code Insight Compliance Library for ongoing detection and matching.

Timely Notification of Vulnerable Components in Your Code

Vulnerabilities in open source projects have recently received a lot of visibility. The Heartbleed and ShellShock vulnerabilities reported in 2014 caused many organizations to re-examine their open source use policy. Since 2009 vulnerability reporting has been part of FlexNet Code Insight. After open source artifacts are identified following scan, they are added to the inventory of third-party components for the project being analyzed (published inventory). At this point, vulnerability information and notification is available within the system. Vulnerability status is visible on the inventory page, and via a vulnerability report. In addition, when an existing inventory item or request gains a new vulnerability, users are notified on the Security Alerts tab in the Web UI and via email.



Filter: In Progress Projects Search:

Project ▲	Audit (does not include files within archives)	Inventory Review	Inventory with Legal / Remediation / Security Issues
Project1	19 of 43 files with indicators reviewed 2 of 35 files without indicators reviewed	Rejected: 1 | Pending: 2 | Approved: 5 Total inventory items: 21 Un-reviewed inventory items: 13	Legal | Open: 0 | Completed: 0 | None: 21 Remediation | Open: 0 | Completed: 0 | None: 21 Security Issues | Open: 0 | Completed: 0 | None: 21

Figure 1:FlexNet Code Insight Dashboard

Extensive Compliance Library and Language Coverage

The FlexNet Code Insight Compliance Library is the basis for binary and source code searches. It contains open source releases continuously collected over the last 12 years, as well as commercial/third-party content. As a result, even if open source components and versions have been removed from the web during this time, they still exist in the FlexNet Code Insight Compliance Library and can be detected during scan.

Information for the Compliance Library is derived from both automated and human collection. Currently the library contains over 12.9 million open source components. After collection, the results are indexed and packaged for use. Updates to the Compliance Library are available on physical media or may be downloaded electronically.

Proven and Scalable Request & Authorization Workflow

FlexNet Code Insight is designed as an end-to-end system for management of open source and third party software. In addition to the comprehensive scanning capability, FlexNet Code Insight also includes request and approval workflow capabilities. Developers can make requests to use open source components in their development, and receive authorization, either automatically, or after review by the appropriate stakeholders in development, legal and security.

Organizations have the opportunity to enforce their use policy at the point of request as well as record and maintain information about the component such as where used, license, modifications, and other relevant data. The request and approval workflow system was developed in cooperation with some of the world's largest software companies and incorporates a number of best practices and specialized capabilities unique to the process of approving and tracking open source use. Capabilities include:

- Immediate vulnerability advisory of requested components, and UI/email alerts for in-use components that gain new vulnerabilities
- Bulk approval capability for requests that are part of the same project or require similar guidance
- Dynamic fields allow for a broader set of workflow processes
- Corporate request view across projects
- Flexible routing with dynamic selection of reviewers
- Legal templates for delivering legal guidance to requestors
- Private fields to maintain attorney-client privilege
- Prioritized component search results with important components on top
- Request history provides visibility across the entire request review process
- Reconciliation of audit results with requested components

Supporting A Vast Range of Languages, Including:

Ada – .ada, .adb, .ads

ASP – .aspx, .ascx

C/C++ – .c, .cc, .cpp, .cxx, .h, .hh, .hpp, .hxx, .m

C# – .cs

Delphi – .pas

Erlang – .erl, .hrl

F# – .fs, .fsi, .fsx, .fsscript, .ml, .mli

Fortran – .f90, .f95, .f03, .f, .for, .f77, .F, .F90, .f08

Go – .go

Java – .java, .jsl, .jsp, .groovy

Javascript – .js, .as, .ts

Lua – .lua

Perl – .perl, .pl, .pm, .prl

PHP – .inc, .php

Python – .py

Ruby – .rb., .rbw, .rbx, .rhtml, .ruby

Scala – .scala

Shellscript – .sh, .bash, .ksh, .csh, .tcsh, .zsh

Swift – .swift

Tcl (Tickle) – .tcl, .tk

Text – No extensions specified bydefault

Verilog – .v, .vh

VHDL – .vhd, .vhdl

Visual Basic – .bas, .vb

Because FlexNet Code Insight is designed as an integrated system, the request and authorization workflow is fully integrated with scanning so that published scan results can be associated with existing requests, or in the event that scanning detects a component without a request, it creates a request for the discovered component.

Designed for Enterprise Environments

FlexNet Code Insight is designed to be installed and used on-site, and has a full set of enterprise-ready features to allow operation within a modern IT environment.

- User Management can be done within FlexNet Code Insight or via interconnection with existing LDAP and Single Sign-On systems and supports a number of user roles with distinct access privileges
- Support for MySQL, Oracle and SQL Server databases, and Windows and Linux operating systems

- Written in Java, and uses Apache Tomcat as the application platform
- Application security is maintained through continuous testing against known attack vectors
- Can be used without connection to the external internet for secure environments

Integration

- REST APIs provide access to resources and data such as automated findings, audit and vulnerability information
- The Jenkins Plugin lets users trigger a FlexNet Code Insight scan as part of the Jenkins build
- Upload to Scan capability lets users quickly upload one or more files for immediate scan and reporting from anywhere at any time
- Source Code Management support includes integration with GIT, TFS, Subversion, Perforce and Clearcase

About Flexera Software

Flexera Software helps application producers and enterprises manage application usage and increase the value they derive from their software. Our next-generation software licensing, compliance, security and installation solutions are essential to ensure continuous licensing compliance, optimize software investments and future-proof businesses against the risks and costs of constantly changing technology. Over 80,000 customers turn to Flexera Software as a trusted and neutral source for the knowledge and expertise we have gained as the marketplace leader for over 25 years and for the automation and intelligence designed into our products. For more information, please go to: **www.flexerasoftware.com**

Recommended System

FlexNet Code Insight utilizes one or more scan servers, a core server and a database server. For single user scanning use the software can be installed on a single system. More commonly, FlexNet Code Insight is deployed for use by multiple users and is designed to scale for this use case, with separate machines or partitions to support the different functions.

Server Hardware:	• 16GB or 32GB RAM minimum, depending on expected load • 750GB free hard disk space *(recommend 1 TB)* • Solid State Drive is recommended for reducing scan time
Recommended Operating Systems:	• RHEL 7.0, 7.2 (64-bit) • Windows 7 Enterprise (64-bit) • Windows Server 2012 Enterprise (64-bit)
Supported Operating Systems:	• RHEL 6.5, 7.0, 7.2 (64-bit) • Ubuntu 14.0.4 • CentOS 6.5 (64-bit) • Windows 7 Enterprise or Professional (64-bit) • Windows 8.1 Enterprise or Professional (64-bit) • Windows Server 2012 Enterprise or Professional (64-bit) • Mac OS (all versions)
Java:	• JDK 7, 8, (64-bit) *(required on Core, Scan Servers)* • JRE 7, 8 (64-bit) *(required on Client Servers)*
Database:	• MySQL 5.6, 5.7 • Oracle 11g, 12c • MS SQL Server 2012

Next Steps:
For more information, call Flexera Software today!
1 (800) 809-5659

Flexera Software LLC
(Global Headquarters):
+1 800-809-5659

United Kingdom (Europe,
Middle East Headquarters):
+44 870-871-1111
+44 870-873-6300

Australia (Asia,
Pacific Headquarters):
+61 3-9895-2000

For more office locations visit:
www.flexerasoftware.com