

KNOW WHAT'S IN YOUR CODE

Code Insight

Manage Open Source License Compliance & Security Vulnerabilities

Key FlexNet Code Insight Facts

- Largest, most comprehensive open-source library with more than 14 million open source components
- Detects components across hundreds of programming languages, binary formats, and frameworks
- Secure on-premises application
- Seamless integration with your development tools
- Allows users to easily create third-party notices
- Compliance library maps over 400,000 component versions to vulnerabilities
- Patented scan technology for both source and binary files
- Efficiently scan as needed while tuning up/down the depth and breadth of analysis

Today, developers are leveraging more than 50 percent of Open Source Software (OSS) in their proprietary applications. That speeds up the time to market drives innovations and revolutionizes the technology world.

In this new environment, data breaches, compliance lawsuits, and security vulnerabilities, are real concerns. FlexNet Code Insight is the end-to-end platform that enables your teams to manage your open source compliance and security needs.

Discover and Track All Open Source Software

FlexNet Code Insight scans your applications to identify open source components in:

- Source code
- Software packages
- Binaries
- Code snippets
- Build dependencies
- Docker images
- Multimedia files

The product also detects licenses, copyright, email/URLs and custom search terms to find evidence of third-party and commercial code.*

You can adjust the depth and breadth of scan and analysis based on your project and risk profile. A quick scan helps you prioritize issues based on a high-level overview. Trigger deep scans where necessary to create a detailed and complete analysis.

** Use custom library data to represent non-OSS third-party and commercial content in your Bill of Materials.*

Identify Security Vulnerabilities & Manage Risk

Identify known vulnerabilities associated with the open source in your applications and get alerts when new vulnerabilities affecting you are reported. Analyze security risks within projects with easy-to-understand dashboards and reports.

FlexNet Code Insight includes a robust framework supporting multiple data sources for vulnerability data, including NVD, RubySec, Debian, RustSec, and advisories from Secunia Research at Revenera.

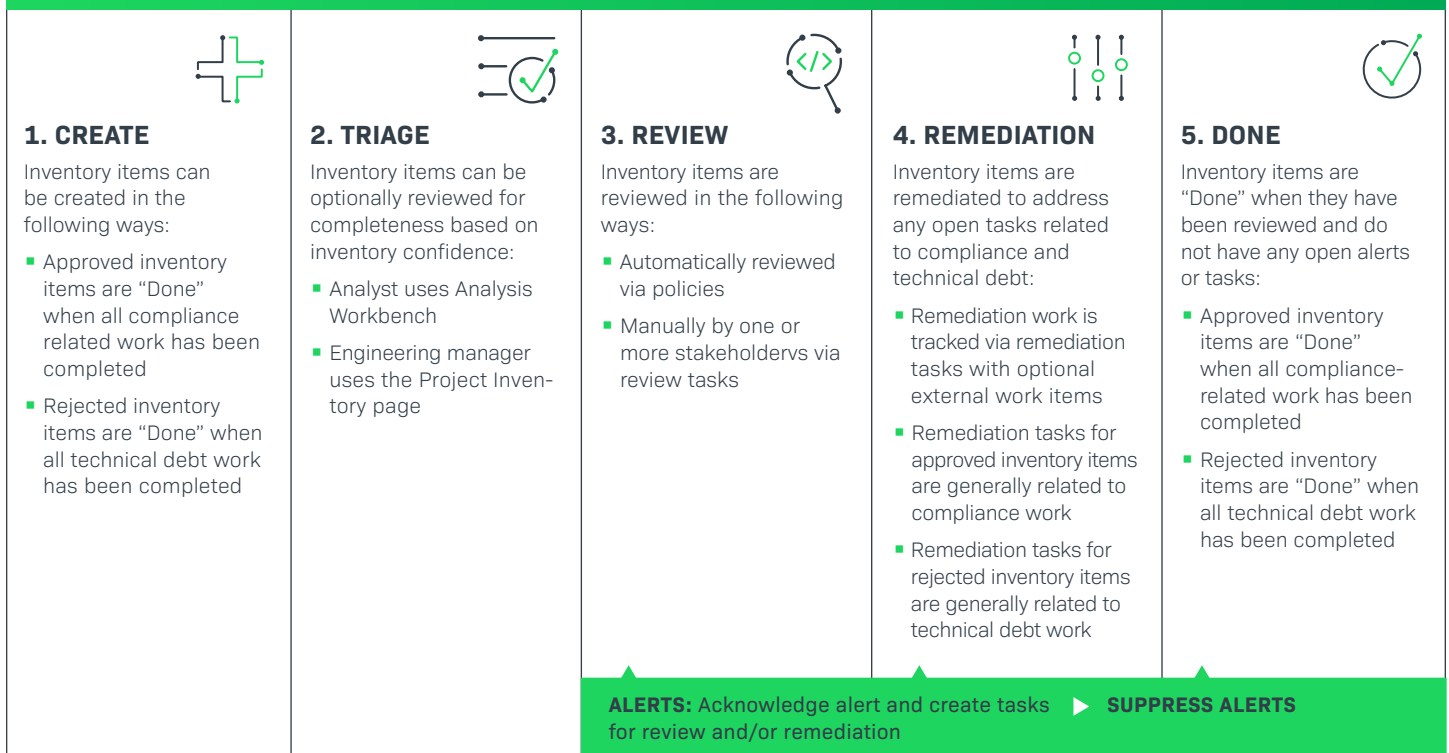
Comply with Open Source Licenses & Manage Obligations

Identify open source licenses and drill down into license details and risk. FlexNet Code Insight automates the creation of an accurate Bill of Materials (BOM) to ship with your products. Automated discovery supports scanning within archives along with direct and transitive dependency reporting for many popular ecosystems.

The FlexNet Code Insight inventory view lists all your components, prioritizes issues, and create tasks for your teams. This enables you to comply with license obligations that come with open source software and protect your IP.

Inventory Lifecycle

Revenera supports a standardized, repeatable process to enhance your inventory management, help you to leverage the power of FlexNet Code Insight, and to ensure you get clean and stay clean.



Supported Programming Languages & Extensions

FlexNet Code Insight supports a host of programming languages, especially the most popular, and scans all artifacts, applies automated detection rules, and performs lookups in the Revenera compliance library.

Programming Languages: Visual Studio, Net, C#, C/C+, CoffeeScript, Go, Groovy, Haskell, Java, JavaScript, Julia, Kotlin, Lua, Matlab, NodeJS, Obj-C, Perl, PHP, PowerShell, Python, R, Ruby, Rust, Scala, Shell, SQL, Swift, and Typescript

Package Formats: .NET (NuGet), DLL/EXE (PE Header), Go (Dep, godep, govendor, glide, trash), Java (Maven/Gradle), JavaScript (Bower), NodeJS (NPM), PHP (Composer), RPM (RPM Header) Ruby (Gem), and Swift/Obj-C (CocoaPods)

Binary Formats: .dlls, .exes, jars (.jar, .ear, .war), RPMs, .sar, .tar., tar. bz, tar.bz2, tar.bzip2, tar.gz, tbz, tgz, war, zip

Seamlessly Integrates into Your Development Lifecycle

Integrate open source scanning into your DevOps environment using FlexNet Code Insight's plugins for Visual Studio, Jenkins, Docker, Gradle, Apache Ant, Apache Maven, Bamboo, GIT, TFS SCM, Eclipse IDE, and Azure DevOps. This allows you to scan your code and identify dependencies from the build environment.

Integrate any external audit data into FlexNet Code Insight and develop your own plugins using the Scan Agent Framework.

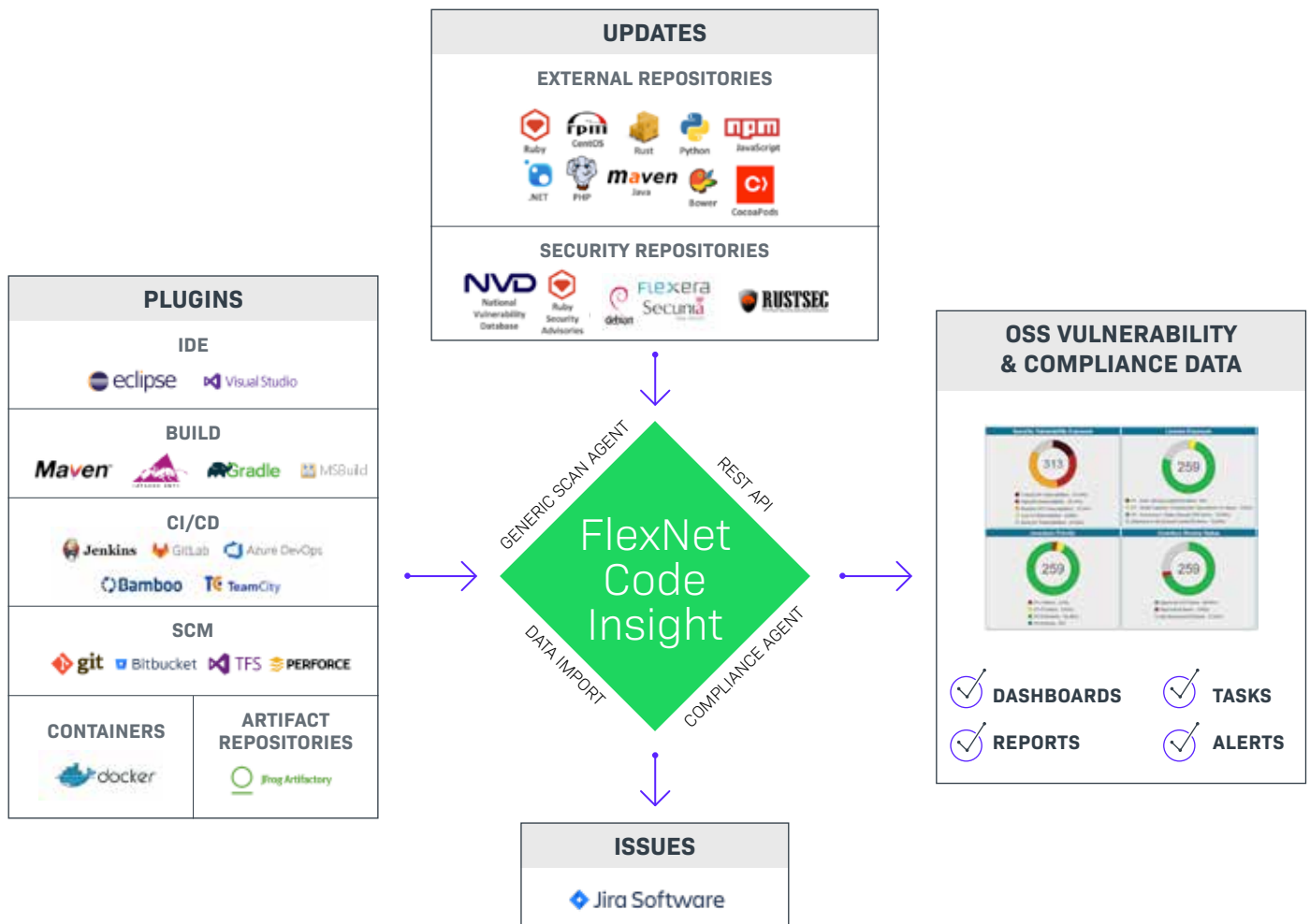
Create custom dashboards and reports with automated findings, audit and vulnerability information using REST APIs.

Policies

Automate the review of commonly used components based on your company license and security policies. Create automated review policies for further control based on component version ranges, security vulnerability scores or severities, or licenses. Developers can select components they intend to use and submit for review. Developers also have access to usage guidance after a component is approved for use, or remediation notes if the component is rejected. You can also automatically create tasks for manual inventory review and remediation.

Devops Integration

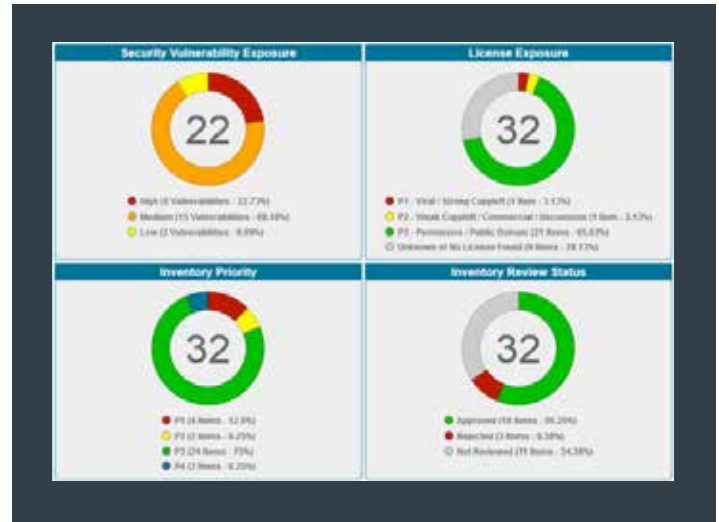
FlexNet Code Insight easily plugs into your build tools, DevOps cycle and your enterprise IT so you can reliably find everything—from packages to code snippets—and remediate issues quickly:



Dashboards & Reporting for Common Queries

Create Third Party Notices and generate reports to stay on top of your open-source code. Quickly answer questions like these and many more:

- Are we exposed to a specific vulnerability?
- Are we exposed to high priority license issues and/or high severity vulnerabilities?
- Where should we focus our limited analysis resources?
- Where are the issues that need attention now?
- Where should we focus our limited analysis resources?
- Where are the issues that need attention now?



Flexible Scan and Analysis Profile Types

Package Discovery

Scan low-risk applications for evidence of all commonly used software packages that are pulled in during the build—via package managers—along with direct and transitive dependencies for a quick health check of your products.

Standard Scan

Package analysis and build dependencies plus evidence of exact file matches, licenses, copyrights, emails, URLs, and search terms.

Comprehensive Scan

Includes everything in Package Discovery and a Standard Scan, in addition to detailed forensic analysis of source code fingerprints to identify case of copy-paste code.