KNOW WHAT'S IN YOUR CODE

Code Insight

Manage Open Source License Compliance & Security Vulnerabilities

Key Code Insight Facts

- Largest, most comprehensive open-source library with more than 16 million open source components
- Detects components across hundreds of programming languages, binary formats, and frameworks
- Secure on-premises application that allows your proprietary code to stay with you
- Seamless integration with your development tools
- Allows users to easily create third-party notices and SBOM reports
- Compliance library maps over 700,000 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
- Use project heirarchy to accurately model your applications and perform incremental analysis from scan to scan

Today, developers are leveraging more than 80 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. Code Insight is the end-to-end platform that enables your teams to manage your open source compliance and security needs.

Build a Complete and Accurate SBOM

Easily and quickly build an accurate open source report of what's in your code. Code Insight scans your applications to identify open source components in:

- Source code
- Software packages
- Binaries
- Code snippets
- Direct and transitive 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 Software Bill of Materials.*

1.800.809.5659 | +44.870.871.1111 | revenera.com

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, and date-based search criteria.

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. Code Insight automates the creation of an accurate Software Bill of Materials (SBOM) to deliver with your products in several formats. Automated discovery supports scanning within archives along with direct and transitive dependency reporting for many popular ecosystems.

The Code Insight inventory view lists all your component versions and licenses, prioritizes issues, and create tasks for your teams. This enables you to comply with license obligations that come

Inventory Lifecycle

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

1. CREATE

Inventory items can be created in the following ways:

- Approved inventory items are "Done" when all compliance related work has been completed
- Rejected inventory items are "Done" when all technical debt work has been completed

2. TRIAGE

Inventory items can be optionally reviewed for completeness based on inventory confidence:

- Analyst uses Analysis Workbench
- Engineering manager uses the Project Inventory page

3. REVIEW

Inventory items are reviewed in the following ways:

- Automatically reviewed via policies
- Manually by one or more stakeholdervs via review tasks

4. REMEDIATION

Inventory items are remediated to address any open tasks related to compliance and technical debt:

- Remediation work is tracked via remediation tasks with optional external work items
- Remediation tasks for approved inventory items are generally related to compliance work
- Remediation tasks for rejected inventory items are generally related to technical debt work

5. DONE

Inventory items are "Done" when they have been reviewed and do not have any open alerts or tasks:

- Approved inventory items are "Done" when all compliance-related work has been completed
- Rejected inventory items are "Done" when all technical debt work has been completed

ALERTS: Acknowledge alert and create tasks for review and/or remediation ▶ **SUPPRESS ALERTS**

Supported Programming Languages & Extensions

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: 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, modules, trash), Java (Maven/Gradle), JavaScript (Bower), NodeJS (NPM), PHP (Composer), RPM (RPM Header) Ruby (Gem), Swift/Obj-C (CocoaPods), .egg, and .crate

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 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 Code Insight and develop your own plugins using the Scan Agent Framework.

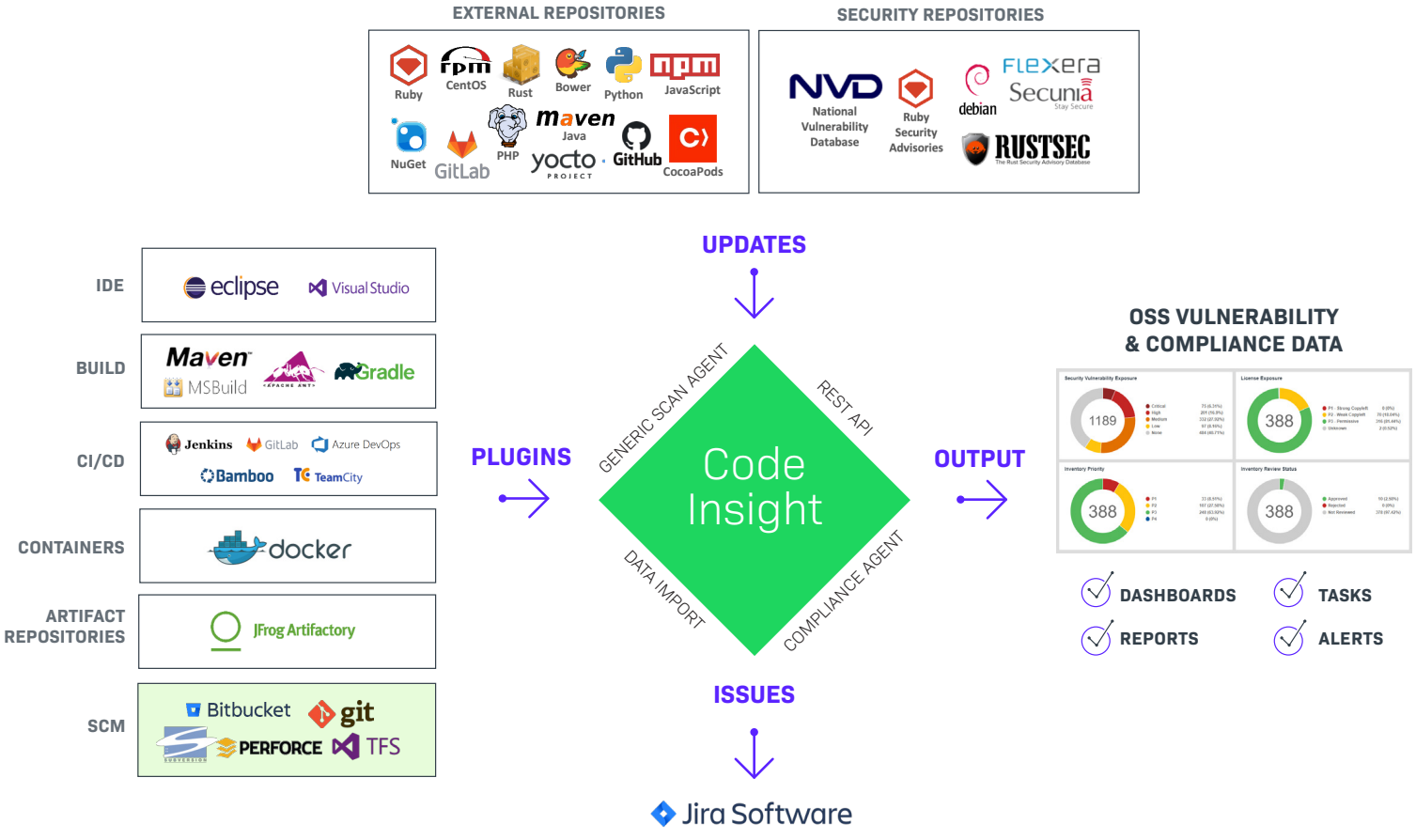
Create custom dashboards and reports with automated findings, audit and vulnerability information using REST APIs.

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.

The "Ins and Outs" of Code Insight

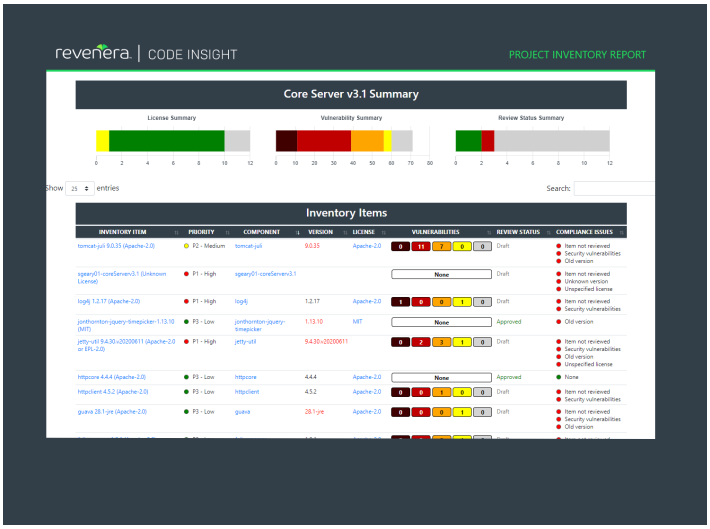
Code Insight easily plugs into your build tools, DevOps cycle and your enterprise IT so you can reliably find everything—from packages to code snippets—and remediate issues quickly:



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.

NEXT STEPS

Visit Revenera to learn more about the value of Code Insight.

LEARN MORE >

Revenera provides the enabling technology to take products to market fast, unlock the value of your IP and accelerate revenue growth—from the edge to the cloud. **www.revenera.com**

revenera
1.800.809.5659 | +44.870.871.1111 | revenera.com