

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 19 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, SBOM reports, and SPDX and CycloneDX reports
- Knowledge base maps over 1.16 million 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.*

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.

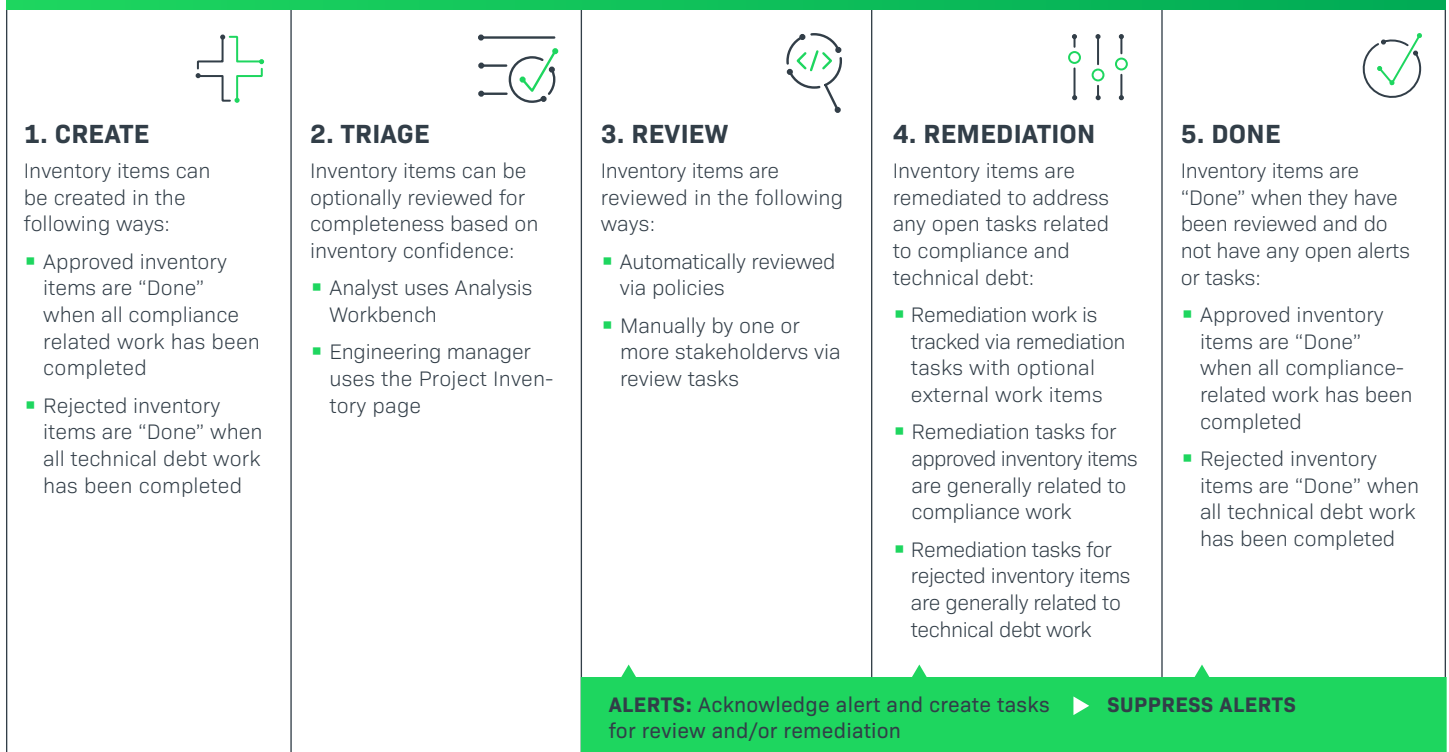
Comply with Open Source Licenses & Manage Obligations

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 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 Code Insight, and to ensure you get clean and stay clean.



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), and Swift/Obj-C (CocoaPods)

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

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.

Now supporting IntelliJ IDE, the OSS Inspector plugin has the following benefits:

- Inspect a Gradle project for OSS components
- Present to the user a full dependency tree of OSS components
- Show OSS components' metadata
- Component, Version, License, Vulnerabilities
- Supports IntelliJ IDE for Java & Kotlin projects using Gradle as build tool
- Free with Reverera SCA offering

The Reverera OSS Inspector plugin enables developers using IntelliJ IDEA (an Integrated Development Environment, or IDE) to examine—within the IDE itself—the licenses and security vulnerabilities associated with the open-source software (OSS) components used in their application code (represented by a project in the IDE). Developers can immediately assess security risks to determine whether they require further review and remediation without leaving the IDE.

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:

