SYNOPSYS®

Code Sight

Find and fix application security defects as you code

Benefits for Developers

Intuitive workflow

- Fix weak code and vulnerable open source dependencies without having to be a security expert
- Get automatic alerts for issues in every file you open, save, and edit, or manually run rapid scans on demand
- Install and start writing more-secure code within minutes

Better code

- Address issues in source code, open source dependencies, API calls, cryptography, infrastructure-as-code, and more
- Instantly see how to fix issues with clear guidance that helps developers become more risk-aware and security-capable
- Become a security champion with access to interactive developer security training from Secure Code Warrior

Increased productivity

- Avoid rework by resolving issues before checking-in code
- Keep moving quickly with IDE-optimized rapid scanning
- Reduce the vulnerability backlog for security teams by eliminating issues before downstream tests

Overview

A developer's role may not be strictly tied to security, but they have a direct impact on the security risk posture of their projects and of the organization. They need insight into risks as they code, and they need to understand how to fix an issue that entered the project inadvertently.

Developers need all this as part of their workflow, without additional steps or tools that may adversely affect productivity.

Code Sight™ is an IDE plugin that helps developers uphold higher standards for application security without switching tools or interrupting their day-to-day tasks. Combining static application security testing (SAST) and software composition analysis (SCA), Code Sight delivers real-time alerts and visibility into

- Security weaknesses (CWEs) in their code
- Known vulnerabilities (CVEs) in open source dependencies
- Insecure infrastructure-as-code (IaC) configurations
- Potential secrets/sensitive data leakage risks
- Vulnerable API usage

Designed for rapid DevOps workflows and CI pipelines, Code Sight can analyze large projects and file structures in seconds, with automation controls to scan whole codebases or modified projects. This allows teams to address defects before checking-in code and avoiding costly rework required when vulnerabilities aren't discovered until downstream testing.

Code Sight complements and improves the effectiveness of other application security testing (AST), alerting development teams to issues detected by other Synopsys AST tools and associated security policy violations. To help developers to quickly fix issues, Code Sight provides detailed remediation guidance directly in the IDE, with recommendations for open source patches, coding best practices, and links to interactive developer security training, powered by Secure Code Warrior.

Benefits for Security

Earlier static analysis

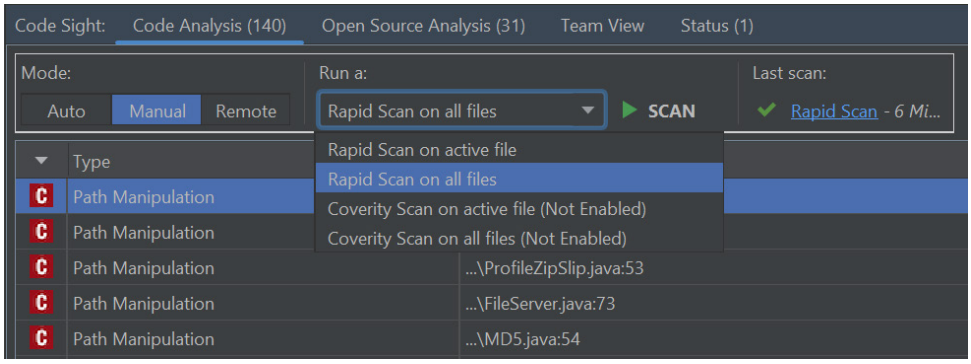
- Analyze source code automatically, as it's written, to detect issues as early as possible.
- Give development teams unified insight into project risks across contributors with the Team View tab
- Remove the subjectivity of risk awareness and security skills with clear fix guidance and interactive developer security training

A smarter supply chain

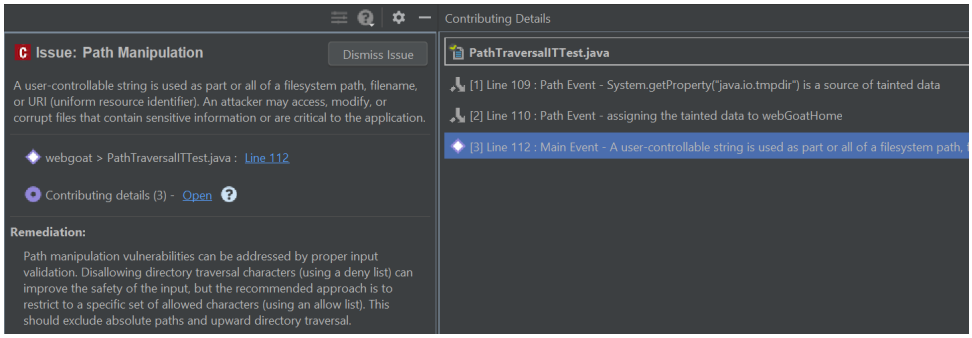
- Identify known vulnerabilities in direct and transitive open source dependencies as developers introduce them
- View vulnerability descriptions, CVE details, and other severity information to quickly prioritize which issues to fix first
- Automatically recommend the next available vulnerability-free or lower-risk version of the component to help developers make smarter, more-secure choices

Flexibility for DevSecOps

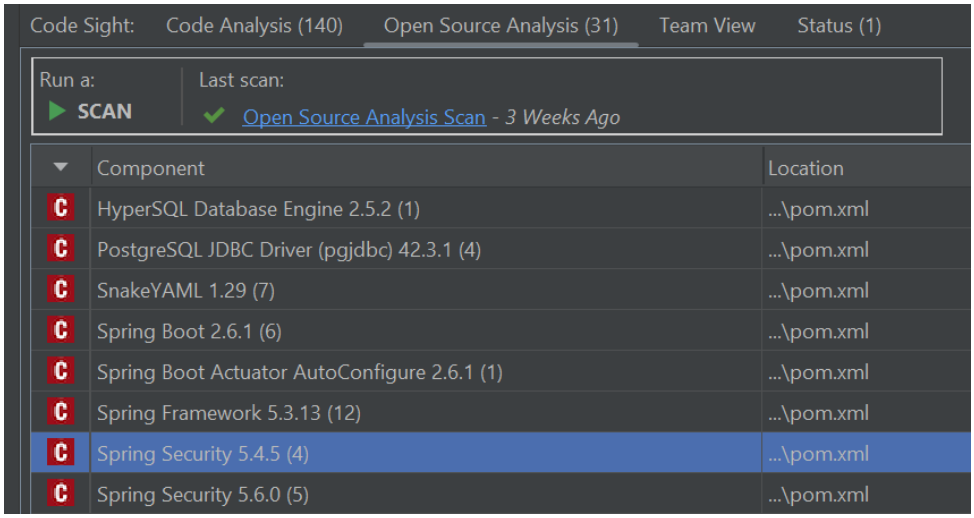
- Get integrated policy violation alerts for connected Coverity® and Black Duck® servers
- Deploy as a standalone solution for secure development or with connected Synopsys AST solutions, like Coverity SAST, Polaris Software Integrity Platform®, and Software Risk Manager

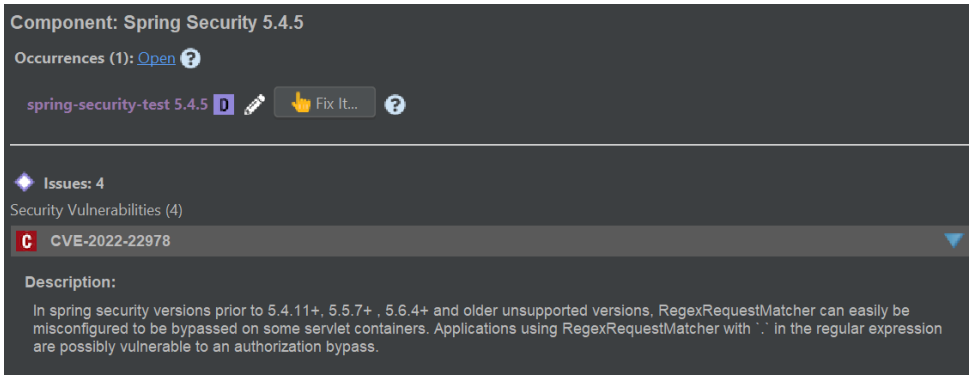


Flexible source code scanning options to balance speed and depth of analysis



Rapid code analysis (SAST), detailed remediation guidance, and links to Synopsys Developer Security Training, powered by Secure Code Warrior





Rapid open source analysis (SCA) with vulnerability details and fix recommendations

Code Sight Standard Edition | Technical Specification

Code Sight Standard Edition supports a broad range of technologies. Some of the popular items it supports include

IDE and languages

IDE

- Eclipse
- IntelliJ
- Visual Studio Code
- Visual Studio

Languages

- Java
- JavaScript
- TypeScript

IaC platforms and file formats

Platforms

- AWS CloudFormation
- ELK
- Helm
- Kubernetes
- Terraform

File formats

- HCL (Terraform)
- HTML
- JSON
- JSX
- Properties
- TOML
- TSX
- Vue
- XML
- YAML

You may access the Synopsys Community for an updated list of languages and frameworks supported by the Code Sight code analysis and open source analysis engines. Additional technical support specifications are available when using the Code Sight extension for Coverity® SAST, Black Duck® SCA, Polaris Software Integrity Platform®, or Software Risk Manager.

This datasheet applies to Code Sight 2023.9.0 and later releases.

SYNOPSYS®

The Synopsys difference

Synopsys provides integrated solutions that transform the way you build and deliver software, accelerating innovation while addressing business risk. With Synopsys, your developers can secure code as fast as they write it. Your development and DevSecOps teams can automate testing within development pipelines without compromising velocity. And your security teams can proactively manage risk and focus remediation efforts on what matters most to your organization. Our unmatched expertise helps you plan and execute any security initiative. Only Synopsys offers everything you need to build trust in your software.

For more information, go to www.synopsys.com/software.