WhiteSource

WhiteSource Native Integrations for Developers' Environments

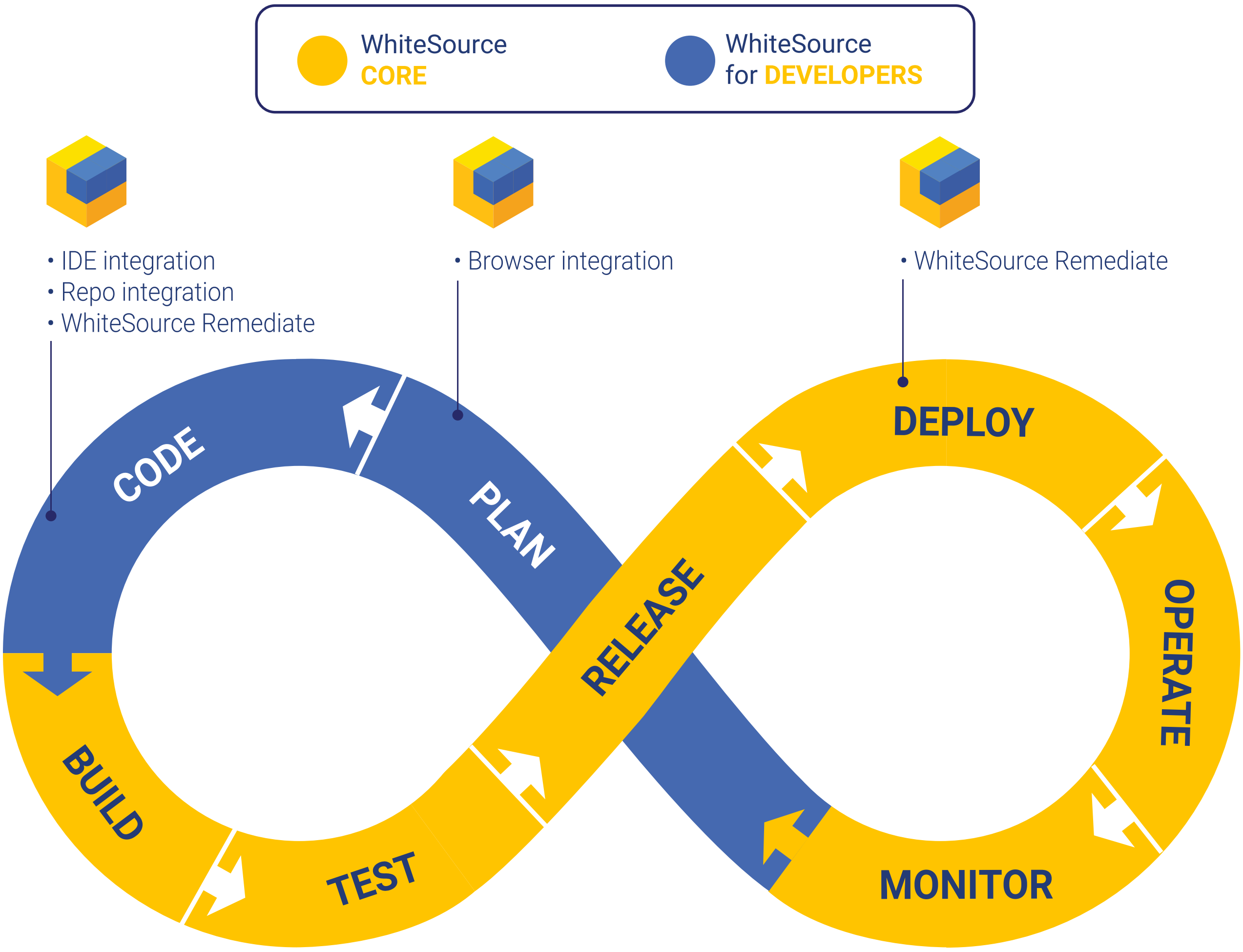
Why Do We Need Developer-Focused Tools?

WhiteSource for Developers was designed to make developers' lives easier when working with open source, enabling them to code faster and more securely.

Integrating into their native development environments, (browsers, IDEs, and repositories), WhiteSource for Developers provides developers with the information they need, when and where they need it, through frictionless integration.

WhiteSource for Developers simplifies dealing with open source components from the earliest stages of development by helping developers choose better open source components, detect vulnerable and problematic components throughout the development lifecycle and automate key elements of the remediation process.

Help Your Developers Work Smarter, Not Harder



The Developer’s Toolbox

REPOSITORY INTEGRATIONS

detect all open source components in developers’ repos on every commit, alert on vulnerabilities and offer suggested fixes within the repo UI. They also allow enforcement of security policies, initiate workflows, and offer a wide range of up-to-date reports and actionable insights on your repository.

The integrations support all major repositories, and empower developers to use open source freely and fearlessly by offering full visibility, with detailed security and remediation information for simpler remediation.

IDE INTEGRATIONS

are lightweight integrations that don’t interfere with the coding experience.

When a vulnerable dependency is detected, developers get real-time alerts within the IDE UI, along with practical remediation guidance.

The IDE integrations help developers minimize the use of an additional application outside of their coding environment or wait until code is committed to receive alerts on vulnerable components.

IJ WS PC

WHITESOURCE REMEDIATE

continuously tracks repositories to identify vulnerable and outdated open source components and automatically generates fix Pull Requests (PRs) with the latest version, including important details and insights to help developers speed up remediation.

By automating the remediation process, developers can save precious time and reduce exposure to known vulnerabilities, significantly improving the security of their code.

BROWSER INTEGRATION

provides developers with a snapshot of an open source component’s security and quality while browsing the web. It identifies package installation references on StackOverflow, Maven Central, RubyGems, and more. Details include known vulnerabilities, license type, quality score, library information and whether the component is currently in use within your organization.

It enables developers to choose better components the first time around, saving time spent on tear and replace in later stages.

Top Benefits

Fuse Security into Developers’ Native Environments

Alert your developers on security issues in their familiar environment, or even their browser, to boost their productivity while improving application security.

Speed Up Processes With Automated Remediation Workflows

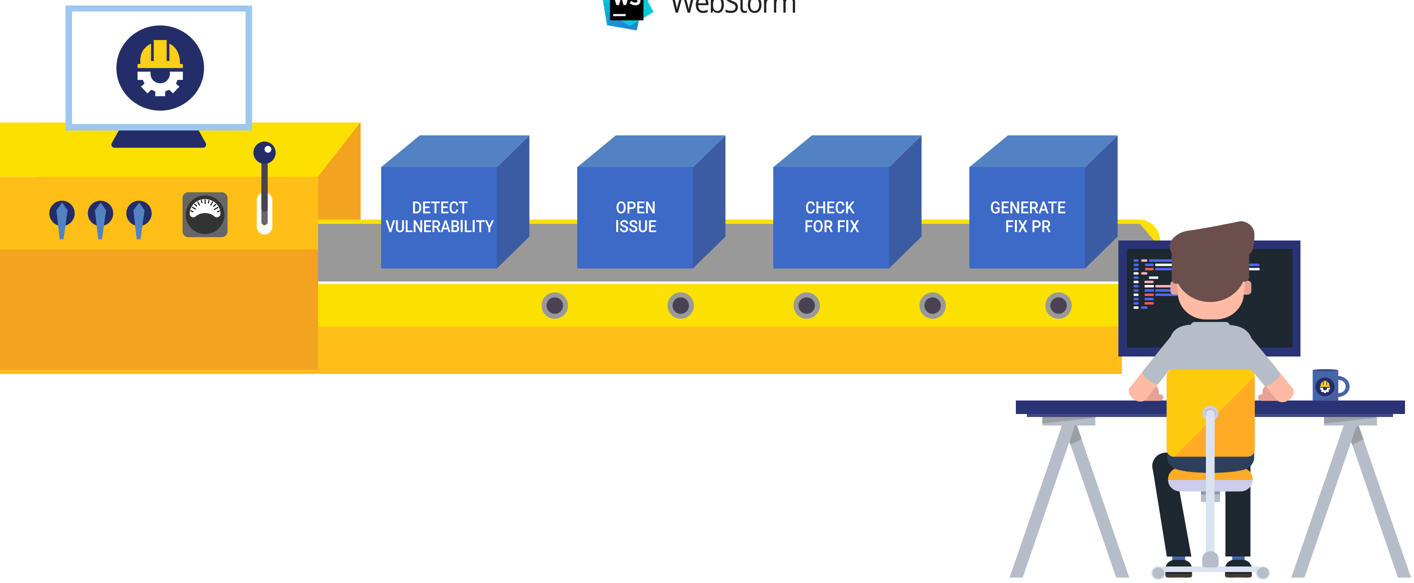
Use automated workflows to replace manual tasks such as detecting known open source vulnerabilities in your projects, tracking newly disclosed vulnerabilities, searching for the right fix, and preparing a fix pull request.

Gain Early Visibility to Prevent Issues

Get real-time visibility over known security vulnerabilities in your open source components as soon as you add them to your code, even before a commit. Review helpful security recommendations early — when they are still easy to fix.

Supported Environments

Browser	IDEs	Repositories
Google Chrome	Visual Studio	GitHub.com
	Code	GitHub Enterprise
	Eclipse	Bitbucket Server
	IntelliJ IDEA	GitLab
	PyCharm	
	WebStorm	


DETECT VULNERABILITY
OPEN ISSUE
CHECK FOR FIX
GENERATE FIX PR