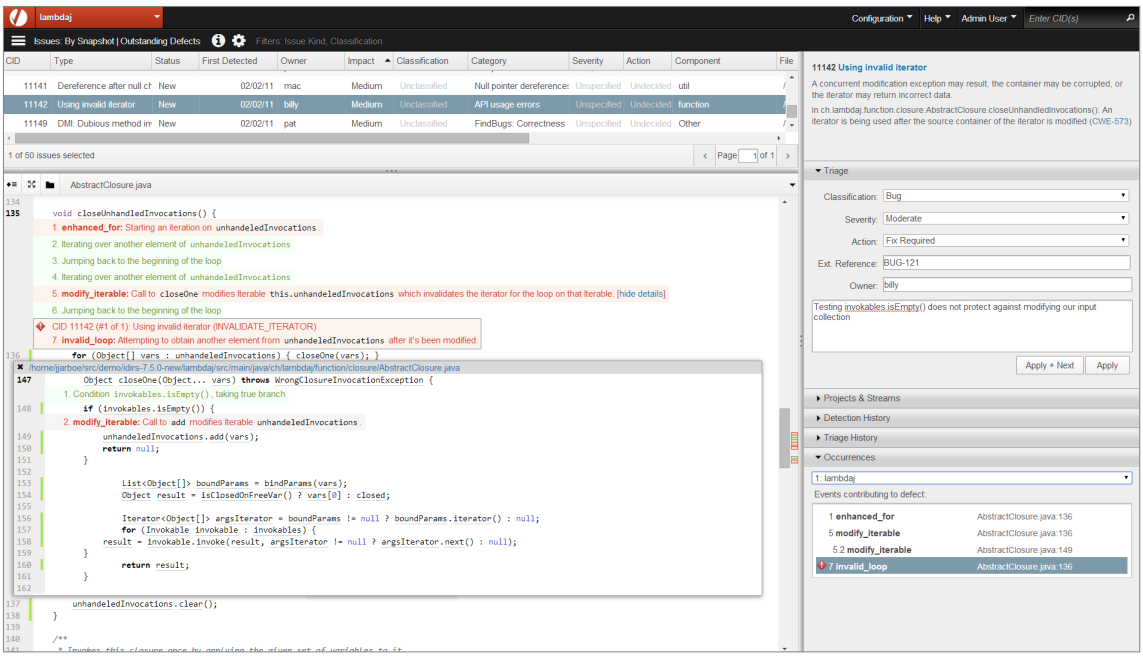
coverity®
A Synopsys Company

DATA SHEET

Coverity Security Advisor

Coverity® Security Advisor identifies critical security defects in the developer workflow with accuracy and actionable remediation guidance, and without requiring deep security expertise.



Actionable remediation guidance helps developers understand how and where to fix critical security defects.

Product Overview

Coverity Security Advisor is part of the Coverity Software Testing Platform, which empowers developers to build testing into the development process at the earliest stage. It surfaces security defects in the developer workflow with accuracy and actionable remediation guidance. This code intelligence helps developers write more secure software by providing visibility into what issues need to be fixed, where to find them and how to fix them. Now critical defects can be addressed during development so they can be corrected before they become security vulnerabilities in production, which ultimately lowers risk and decreases project costs.

Key Features

Intelligent Code Analysis

Coverity Security Advisor finds critical security defects in Java web applications by leveraging sophisticated, patented analysis techniques for accurate defect detection. These techniques include interprocedural dataflow analysis to find complex issues that cross function, file and class boundaries: Boolean satisfiability solvers to improve accuracy through bit-accurate analysis; false-path pruning to understand data dependencies in the code and eliminate infeasible paths; statistical programming to detect coding patterns and learn programmer's intent to reduce "noise" in results; and design-pattern intelligence to understand patterns and programming idioms that are incorporated into the analysis.

Coverity analysis innovations for Java web application security include:

- **Enterprise Framework Analyzer:** Augment source code analysis by providing a deep understanding of modern web applications, including dependency injection, entry points and the Model-View-Controller (MVC) paradigm.

ADDRESS SECURITY AT THE SOURCE

- Identify and remediate critical OWASP Top 10 vulnerabilities
- Combine Static Application Security Testing (SAST) with Interactive Application Security Testing (IAST) through integration with NT Objectives for high-confidence results
- Understand what issues to address, where to find them and how to fix them with precise and prescriptive remediation advice

- **White Box Fuzzer:** Automatically validate that data-sanitization routines perform sufficient sanitization of untrusted data and are used in the right context.

Coverity Security Advisor finds critical security issues such as SQL injection, XSS and other OWASP Top 10 issues. Because developers receive accurate results, they don't have to waste time chasing down false positives or false negatives. Instead they can focus their efforts on fixing real, relevant and critical issues.

Efficient Issue Management

Coverity Connect is the collaborative issue management interface that efficiently manages all issues surfaced by the Coverity analysis engines from triage to resolution within a unified workflow. Key features for automated issue management include:

- Easily filter and view critical security related issues such as OWASP Top 10, PCI and other security related issues.
- Multiple patented analysis techniques to minimize false positives.
- Source code navigation to identify the exact path to the defect.
- Impact mapping to identify every occurrence of the defect across shared code.
- CWE-compatible mapping and knowledge base for each defect.
- Automatic assignment of defects to the appropriate developer.

Remediation Engine

A key reason legacy security tools fail in development is because they require security expertise and lack actionable remediation guidance. Through a deep understanding of the source code and application framework, the Coverity Security Advisor remediation engine provides precise guidance about the right way to fix a defect and the best place to fix it in the code. This ensures your developers remediate defects faster, and "get it right the first time."

Integration with the Developer Workflow

Coverity Security Advisor provides bi-directional integration with existing lifecycle tools to make software testing a natural part of the development lifecycle, including:

- Integrated development environments (IDEs) to surface and remediate defects before code check-in, right at the desktop.
- Source control management to map defects to code changes and responsible developers.
- Bug tracking to link security defects to your overall defect-management process.
- Build and continuous integration to automatically test for quality defects with every build or as part of an Agile process.

Static and Interactive Application Security Testing (SAST and IAST)

For IAST, Coverity has partnered with NT OBJECTives (NTO), and the results from NTOSpider can be automatically correlated with the Coverity SAST findings and easily integrated into the development workflow through Coverity Connect.

Supported Platforms

Coverity Security Advisor for Java

Platform Support	IDE Support
• Linux • Mac OS X • Solaris • Windows	• Eclipse v3.5+ • IBM Rational Team Concert

Coverity Connect

Server Platform Support	Browser Support
• Linux • Mac OS X • Solaris • Windows	• Internet Explorer 8, 9, 10 and 11 • Firefox: Mozilla supported versions • Google Chrome: Google supported versions • Safari 5.1.5 or later

coverity®
A Synopsys Company

For More Information
www.coverity.com
Email: info@coverity.com

Coverity Inc. Headquarters
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: (800) 873-8193
International Sales: +1 (415) 321-5237
Email: sales@coverity.com