SYNOPSYS®

Coverity Static Analysis

Coverity is an accurate and comprehensive static analysis and static application security testing (SAST) solution that finds critical software defects and security vulnerabilities in code as it's written

Overview

Coverity, our static analysis solution, helps reduce your software quality and security risks and lowers overall software development costs by identifying critical quality defects and potential security vulnerabilities during development. It provides reliable, actionable remediation guidance based on patented analysis techniques, a decade of research and development, and analysis of trillions of lines of proprietary and open source code.

Key features

Depth and accuracy of analysis

- Through a deep understanding of the source code and the underlying frameworks, Coverity provides highly accurate actionable analysis results so developers do not waste time on a large volume of false positives. This enables them to build security into the development life cycle at the speed of agile CI/CD workflows.
- Coverity provides full path coverage, ensuring that every line of code and every potential execution path is tested. It uses multiple patented techniques for deep, accurate analysis.
- Coverity integrates into your build system to provide a high-fidelity representation of your source code and its behavior.
- Security teams can analyze many languages just by pointing Coverity to project source code (i.e., without needing to do a build).

Speed and scale of analysis

Coverity was built from the ground up to fit into any existing workflow, with the following capabilities:

- Parallel analysis allows Coverity to run on up to 16 cores simultaneously and delivers up to a 10X performance improvement over serial analysis.
- Fast Desktop Analysis and Incremental Analysis accelerate analysis by reanalyzing only code that has changed or been affected by a change, instead of the entire codebase each time.
- Coverity scales to accommodate thousands of developers in geographically distributed environments and can analyze projects with more than 100 million lines of code with ease.

Address security at the source

- Arm your developers with the information they need to troubleshoot and fix critical defects quickly and efficiently.
- Build quality and security into development to reduce the cost of rework and delayed time to market resulting from defects found late in the cycle.
- Reduce the risk of costly and brand-damaging software failures and security breaches in the field or in production.

Software development life cycle (SDLC) integration

- Coverity can be rapidly integrated with critical tools and systems that support the development process, such as source control management, build and continuous integration, bug tracking, and application life cycle management (ALM) solutions, as well as integrated development environments (IDEs).
- The open platform allows developers to import third-party analysis results into the workflow to view and manage all types of defects in the same way, with a single view of software defects and risks.

Efficient issue management and remediation

- With Coverity Connect, the platform's collaborative issue management interface, developers get actionable information and precise remediation guidance, which shows them the right way to fix a defect and the best place in the code to fix it without requiring deep security domain expertise. Synopsys eLearning customers can also see links to relevant courses associated with specific CWEs found in their code to get better insight into vulnerabilities and immediate security training when they need it.
- Coverity Connect provides source code navigation to highlight the exact path to a defect and automatically identify every occurrence of the defect across shared code.
- Defects can be automatically assigned to the appropriate developer for resolution, and users can quickly view all outstanding issues related to security, OWASP Top 10, CWE, and PCI DSS, as well as quality, MISRA, CERT C/C++, and AUTOSAR.

Expanded standards compliance and vulnerability detection

Coverity Extend is an easy-to-use software development kit (SDK) that allows developers to detect unique defect types. The SDK is a framework for writing program analyzers, or checkers, to identify custom or domain-specific defects. Coverity CodeXM is a domain-specific functional programming language that enables developers to develop their own custom checkers easily. These customized checkers support compliance with corporate security requirements and industry standards or guidelines.

Ability to drive adoption and mitigate risk

With Coverity Policy Manager, you can define and enforce consistent standards for code security as well as quality and testing across development teams. It provides visibility into which teams, projects, and components are compliant with these standards and can create measurable stage gates based on predefined criteria regarding defects and testing. Using customizable views, you can select development metrics and thresholds that align with specific objectives for embedded, enterprise, and mobile applications.

Supported languages

- C/C++
- C#
- Java
- JavaScript
- PHP
- Python
- .NET Core
- ASP.NET
- Objective-C
- JSP
- Node.js
- Ruby
- Android
- Swift
- Fortran
- Scala
- VB.NET
- iOS
- TypeScript

Supported frameworks

Coverity supports over 50 different frameworks for Java, JavaScript, C#, and other languages.

Java

- Android SDK
- Apache Shiro
- Axis
- DWR
- Enterprise Java Beans (EJBs)
- GWT
- Hibernate
- iBatis
- Java Persistence API (JPA)
- Javax.websocket
- JAX RS
- JAX WS
- JEE
- JSF/Facelets
- JSP and JSP Standard Tag Library (JSTL)
- Restlet
- Spring Boot
- Spring Framework
- Struts
- Terasoluna
- Tiles
- Vert.x
- WS XML-RPC

C#

- ASP.NET MVC
- ASP.NET ASMX Web Services
- ASP.NET Web API
- ASP.NET Web Forms
- ASP.NET Core
- ASP.NET Core MVC
- WCF services
- Razor templates

JavaScript/TypeScript

Client-side

- HTML5 DOM APIs / Ajax
- jQuery
- AngularJS
- Angular
- Vue
- React / Preact
- Backbone
- Socket.IO
- Bootstrap
- Mithril

Server-side

- Node
- Express
- Hapi
- Koa
- Mean.io
- SAP XS Classic and Advanced
- Socket.IO
- Vue server-side rendering
- Angular server-side rendering (Express and Hapi engines)
- React server-side rendering (Next.js)
- Passport

Template engines

- Nunjucks
- Consolidate
- Haml
- Marko
- Hogan
- Vision
- Koa-views

Template engines that support JS template DA

- EJS
- Handlebars
- Swig
- Pug
- Jade

Major libraries

- Underscore / Lodash
- Axios
- Sequelize
- Request
- Mongoose / MongoDB

PHP

- Symfony

Python

- Flask
- Django

Ruby

- Ruby on Rails

Supported platforms

- Windows
- Linux
- Mac OS X
- Solaris
- AIX
- HP-UX
- NetBSD
- FreeBSD

SDLC integration

SCM

- AccuRev
- Apache Subversion (SVN)
- CVS
- Git
- Mercurial (Hg)
- Perforce Helix
- Team Foundation Server SCM

IDE/CI

- Android Studio
- Eclipse
- IBM Rational Team Concert
- IntelliJ IDEA, WebStorm, RubyMine, PhpStorm, PyCharm
- MS Visual Studio
- QNX Momentics
- Team Foundation Server
- Wind River Workbench
- Jenkins

Issue tracking

- Jira
- Bugzilla

Supported compilers

- ARM C/C++
- Borland C++
- CEVA-XC4500
- Clang
- Cosmic C
- Freescale CodeWarrior
- GNU GCC/G++
- Green Hills C/C++/EC++
- HI-TECH PICC
- HP aCC
- IAR C/C++
- IBM AIX
- IBM XLC
- Intel C++
- JDK for Mac OS X
- Keil compilers
- Marvell MSA
- MPLAB XC8
- OpenJDK
- QNX C/C++
- Renesas C/C++
- SNC C/C++
- SNC GNU C/C++
- Sony ORBIS SDK
- Sony PS4
- STMicroelectronics GNU C/C++
- STMicroelectronics ST Micro C/C++
- Sun (Oracle) CC
- Sun/Oracle JDK
- Synopsys MetaWare C and C++
- TASKING for ARM Cortex
- TI Code Composer
- Visual Studio
- VisualDSP++
- Wind River C/C++

(This list is not exclusive)

Critical checks

- API usage errors
- Best practice coding errors
- Buffer overflows
- Build system issues
- Class hierarchy inconsistencies
- Code maintainability issues
- Concurrent data access violations
- Control flow issues
- Cross-site request forgery (CSRF)
- Cross-site scripting (XSS)
- Deadlocks
- Error handling issues
- Hard-coded credentials
- Incorrect expression
- Insecure data handling
- Integer handling issues
- Integer overflows
- Memory—corruptions
- Memory—illegal accesses
- Null pointer dereferences
- Path manipulation
- Performance inefficiencies
- Program hangs
- Race conditions
- Resource leaks
- Rule violations
- Security best practices violations
- Security misconfigurations
- SQL injection
- Uninitialized members

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle.

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

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

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com

SYNOPSYS®
Silicon to Software™

11/28/18.ds-coverity-static-analysis.