SYNOPSYS®

Coverity
Static Analysis

Quickly find and fix critical security and quality issues as you code

Benefits

- **Get improved visibility into security risk.** Cross-product reporting provides a holistic, more complete view of a project's risk using best-in-class AppSec tools.
- **Deployment flexibility.** You decide which set of projects to do AppSec testing for: on-premises or in the cloud.
- **Shift security testing left.** Developers get high-fidelity incremental analysis results in seconds as they code, so they can fix any issues prior to the build-test phase.
- **Support developers.** Enable your teams to fix software defects quickly, easily, and correctly by supplying all the context, details, and advice they need to understand how to fix issues.
- **Context-specific eLearning** (available to eLearning customers) specific to CWEs identified in developers' own code provides immediate security training when they need it. Developers don't need to be security experts.

Overview

Coverity® gives you the speed, ease of use, accuracy, industry standards compliance, and scalability that you need to develop high-quality, secure applications. Coverity identifies critical software quality defects and security vulnerabilities in code as it's written, early in the development process when it's least costly and easiest to fix. Precise actionable remediation advice and context-specific eLearning help your developers understand how to fix their prioritized issues quickly, without having to become security experts. Coverity seamlessly integrates automated security testing into your CI/CD pipelines and supports your existing development tools and workflows. Choose where and how to do your development: on-premises or in the cloud with the Polaris Software Integrity Platform™ (SaaS), a highly scalable, cloud-based application security platform. Coverity supports 22 languages and over 70 frameworks and templates.

Coverity includes Rapid Scan, a fast, lightweight static analysis engine that can be used to scan web and mobile applications, microservices, and infrastructure-as-code (IaC) configurations. Rapid Scan runs automatically, without additional configuration, with every Coverity scan and can also be run as part of full CI builds with conventional scan completion times. Rapid Scan can also be deployed as a standalone scan engine in Code Sight™ or via the command line interface, as well as in automated build pipelines, For this use case, Rapid Scan provides actionable early results in seconds for most projects. It's easy to use: simply point to a directory or Git repository—no setup is required. Broad support for platforms and file formats makes it easy to scan IaC configuration files. API and configuration checkers can help identify API misuse and vulnerable configurations in settings files. This is ideal for developers who want immediate analysis feedback, while they are coding and with every code commit. Support for multiple analysis output formats (SARIF, JSON, and console) as well as GitHub Actions and GitLab CI provides pipeline scan automation and issue management support. Rapid Scan can also assign issues to a policy file to automatically break builds.

Key features

Fast and accurate analysis

- With the Code Sight™ integrated development environment (IDE) plugin, developers get accurate analysis in seconds in their IDE as they code. Coverity gives developers all the information they need to fix identified issues including descriptions, categories, severity, CWE data, defect location, detailed remediation guidance, and dataflow traces, as well as issue triage and management features within their IDE.
- Coverity's Point and Scan desktop application enables users to onboard applications (including an IaC build capture feature) simply by pointing to the source code. For development teams that prefer a command line interface, the Coverity CLI feature

provides similar functionality.

Comprehensive reporting and compliance visibility

Coverity on Polaris provides organizations with a holistic view of their applications' risk posture at different software development life cycle (SDLC) stages.

- Security teams can get a centralized aggregated risk profile of their entire application portfolio. APIs enable importing results into other risk reporting tools.
- You can filter identified vulnerabilities by category, view trend reports, prioritize remediation of vulnerabilities based on criticality, and manage security policy compliance (e.g., OWASP Top 10, CWE Top 25, and PCI DSS) across teams and projects.
- "Issues over time" reports show severity levels over different timeframes and give you immediate information about the security posture of your projects. PDF report downloads allow auditors to maintain detailed compliance records.

In addition, Coverity provides best-in-class identification of code quality issues for C/C++ and the most comprehensive coverage of standards related to safety, security, and reliability (e.g., MISRA®, CERT C/C++, CERT Java, DISA STIG, ISO 26262, ISO/IEC TS 17961, and AUTOSAR®), as well as quality issues described in Nvidia's CUDA C++ guidelines.

Enterprise scalability and agility

- With Coverity on Polaris, organizations don't need to install and maintain costly on-premises equipment but can elastically scale their application security testing to meet their growing business needs.
- Polaris setup is as simple as logging into a URL, then downloading and installing the command line interface (CLI) or running it through your CI workflows to start analysis of your source code.
- Since the Coverity analysis engines run on a highly available cloud platform, Coverity on Polaris can easily scale to accommodate thousands of developers and projects and handle millions of issues with high performance and uptime.

Software development life cycle integrations

- The Code Sight plugin requires zero configuration and can be downloaded from the marketplace websites for Visual Studio, Visual Studio Code, Eclipse, IntelliJ, WebStorm, PyCharm, PhpStorm, and RubyMine.
- Coverity also has legacy native integrations for IDEs (e.g., Visual Studio, Eclipse, IntelliJ, RubyMine, Wind River Workbench, and Android Studio), source code management (SCM) solutions, issue trackers (e.g., Jira and Bugzilla), CI build tools (e.g., Jenkins and Azure DevOps), and application life cycle management (ALM) solutions.
- REST APIs are available to support other build automation solutions as well as importing analysis results into other enterprise or custom tools.
- Coverity on Polaris provides additional plugins and integrations for automated cloud-based security testing during development and pre-deployment stages.
- REST APIs are available for importing analysis results into security and risk reporting tools. Refer to the Polaris datasheet for additional information.

Comprehensive issue management dashboards

- Development managers are able to create "issues over time" trendline charts showing overall security risk and compliance to industry standards (e.g., OWASP Top 10 and CWE Top 25) and how individual developers or entire project teams are doing in clearing their prioritized issues.
- You can easily view reporting dashboards of Industry Recognized Priority Lists, Top 5 Issues Types, and Technical Risk Indicators so that you can focus on issues that matter most to your organization and prioritize them.
- Predefined filters allow you to filter and group issues by CWE, standards taxonomy, priority list, risk indicator, path, and individual developer owners.

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.

Coverity Static Analysis | Technical Specification

Supported languages and platforms

- Apex
- C/C++*
- C#*
- CUDA
- Java*#
- JavaScript*#
- PHP*#
- Python*
- .NET Core
- ASP.NET
- Objective-C
- Go
- JSP
- Ruby*
- Swift*#
- Fortran
- Scala
- VB.NET
- iOS
- Android
- TypeScript#
- Kotlin

* These languages are currently supported by Coverity's Point and Scan desktop application and the Coverity CLI feature.
# These languages are supported by Rapid Scan to scan for security vulnerabilities in source code.

Supported IaC platforms and file formats

Platforms

- Terraform
- AWS CloudFormation
- Kubernetes
- Helm
- ELK

File formats

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

Cloud deployment support

- Coverity Connect can be run in containers in AWS and GCP public clouds
- Support for cloud-native technologies: Docker and Kubernetes

Supported frameworks

Coverity supports over 70 different frameworks for Java, JavaScript, C#, and other languages. Coverity also supports security modeling of major cloud provider API frameworks for cloud-native JavaScript apps that interact with AWS services (EC2, S3, DynamoDB, IAM) and Google Cloud Storage APIs (GCP).

Java

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

C#

- ASP.NET Core MVC/ASP.NET MVC
- ASP.NET Core Web API
- ASP.NET ASMX Web Services
- ASP.NET Web Forms
- Identity Server
- MassTransit
- Razor templates
- WCF Services

JavaScript/TypeScript

Client-side

- Angular
- Angular JS
- Apache Cordova
- Backbone
- Bootstrap
- Ember
- HTML5 DOM APIs/Ajax
- jQuery
- Mithril
- React/ Preact
- Socket.IO
- Swig
- Vue

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

Template engines
- Consolidate
- doT.js
- EJS
- Handlebars
- Hogan
- Jade
- koa-views
- Lodash (templating)
- Marko
- Mustache
- Nunjucks
- Pug
- Swig
- Twig
- Underscore (templating)
- Vision

Major libraries
- Axios
- Google Cloud APIs (Storage)
- Mongoose / MongoDB
- Request
- Sequelize
- Sqlx
- Swashbuckle
- Underscore / Lodash

GO
- Echo

PHP
- Symfony

Python
- Flask
- Django

Ruby
- Ruby on Rails

Rapid Scan IaC Frameworks
- Android
- Apache Cordova
- Apache Kafka
- Apache Struts
- Apache Zookeeper
- Apollo GraphQL
- AWS Cloudformation
- Consul
- Express
- Grails® framework
- GraphQL
- Istio
- Jakarta Server Faces
- Java/Jakarta EE
- Kubernetes
- mybatis
- NodeJS
- OpenAPI
- Postman
- RabbitMQ
- React
- Socket.IO
- Spring
- Terraform
- Vue.js

Supported platforms
- Windows
- Linux
- Mac OS X
- Solaris
- AIX
- NetBSD
- FreeBSD

SDLC native integrations

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

Legacy IDEs
- IBM Rational Team Concert
- QNX Momentics
- Wind River Workbench

CI build servers
- Jenkins
- Azure DevOps Server

Code Sight supported IDEs*
- Visual Studio for VB.NET, C#, C/C++, JavaScript, PHP, Python, Ruby, TypeScript
- Visual Studio Code for C# (.NET Core), C/C++, Java, JavaScript, PHP, Python, Ruby, TypeScript
- Visual Studio Code (Rapid Scan) for Java, JavaScript, and TypeScript
- Eclipse for Java, JavaScript, C/C++, PHP, Python, Ruby, TypeScript
- IntelliJ for Java, JavaScript, PHP, Python, Ruby, TypeScript
- WebStorm for JavaScript, TypeScript
- PyCharm for Python
- PhpStorm for PHP
- RubyMine for Ruby

Issue tracking
- Jira
- Bugzilla

Supported compilers
- Analog Devices Blackfin
- Analog Devices SHARC
- Analog Devices TigerSHARC
- ARM C/C++
- Borland C++
- CEVA BXx
- CEVA XC16
- CEVA-X2
- CEVA-XC4500
- Clang
- Cosmic C
- Freescale CodeWarrior
- GNU GCC/G++
- GHS PowerPC on Windows
- Green Hills C/C++/EC++
- HI-TECH PICC
- IAR C/C++
- IBM AIX
- IBM XLC
- Intel C++ for Windows
- JDK for Mac OS X
- Keil compilers
- Marvell MSA
- MPLAB XC8
- Nvidia CUDA Compiler (NVCC)
- OpenJDK
- QNX C/C++
- Renesas C/C++

- SNC C/C++
- SNC GNU C/C++
- SONY PS4 SDK
- STMicroelectronics GNU C/C++
- STMicroelectronics ST Micro C/C++
- Sun (Oracle) CC
- Sun/Oracle JDK
- Synopsys MetaWare C and C++
- Tasking for ARM Cortex and TriCore
- TI Code Composer
- Visual Studio
- 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

* For the latest CodeSight and supported IDE version numbers, see https://dev.sig-docs.synopsys.com/codesight/topics/support_matrix/r_code_sight_support_matrix.html

The latest Rapid Scan analysis engine announcements and release updates (standalone use case) can be found here.

This datasheet applies to Coverity 2021.12.0 and later releases.

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.

For more information about the Synopsys Software Integrity Group, visit us online at www.synopsys.com/software.

Synopsys, Inc.
690 E Middlefield Road
Mountain View, CA 94043 USA

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