CODESonar®

DATASHEET

Static Application Security Testing

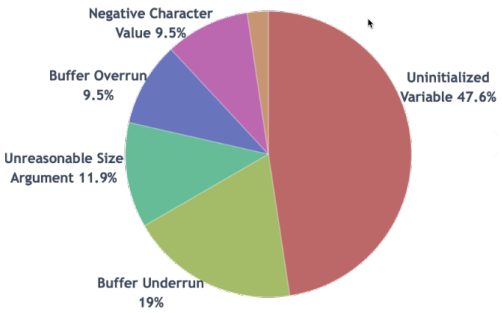
CodeSonar is a static application security testing solution (SAST) that helps you find and understand security and quality defects in your source code or binaries.

Accelerate Application Security

Software teams are under constant pressure to deliver more content, with higher complexity, in shorter timeframes, and with increased security and quality. CodeSecure has been a leader in this field for over 15 years, with CodeSonar delivering multi-language capabilities for enterprises where software security and quality matter.

- **Language Support**. CodeSonar supports many popular languages, including C/C++, Java, C#, Kotlin, Python, Go, Rust, JavaScript, and TypeScript.
- **Security**. CodeSonar checks for the use of tainted data, buffer issues, dangerous memory access, integer and floating-point overflow, and other common security coding errors.
- **Deep Analysis**. CodeSecure builds a highly accurate abstract representation of your application and uses that to examine all the paths through your code to find problems and vulnerabilities. With this deep insight into issues, your team can decide when and how to resolve warnings with confidence.

Buffer over-and under-runs
Copy-paste error
Memory leak
Dangerous function
Cast and conversion
Concurrency problems
Unused parameter
Tainted data value
Command injection
Ignored return value
Null pointer dereference
And hundreds more



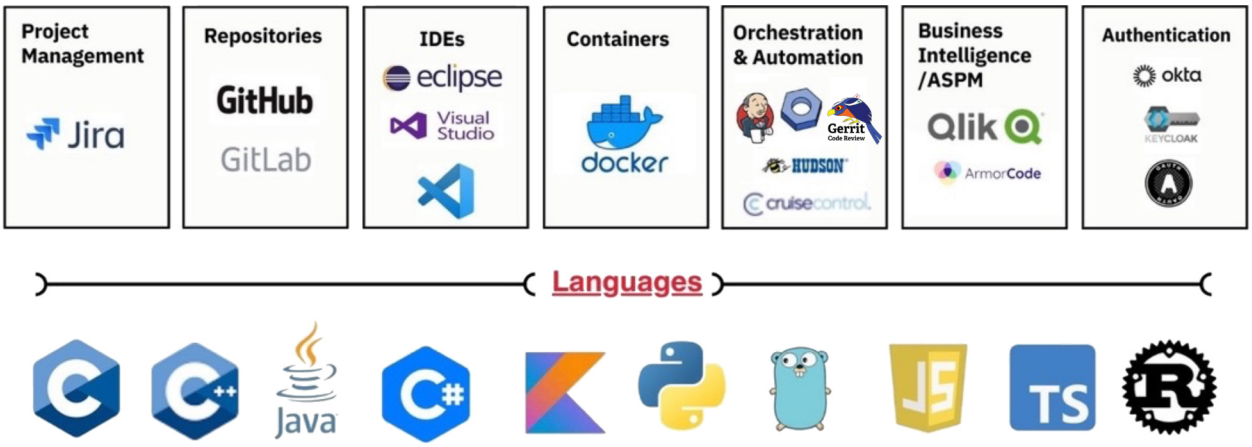
- **Code Quality**. CodeSonar detects memory leaks, dangerous memory access, and other common causes of low-quality code.
- **Scale**. Analyze projects of any size.
- **Integrations**. CodeSonar ships with integrations to most popular development tools. It also supports OASIS SARIF for the exchange of information with other tools in your DevSecOps environment.
- **Code Performance**. CodeSonar detects code that negatively affects performance, such as unnecessary tests for *nullness*, the creation of redundant objects, or superfluous memory writes.
- **Reporting**. CodeSonar provides built-in reports for standards, such as MISRA, OWASP, and CWE. CodeSonar also includes a custom report builder your organization can use to develop a better understanding of the quality and security of your software projects. Export in CSV, PDF, HTML, or XML so you can work the way you want to.

CODESECURE

U.S. Sales: 703.728.8511
International Sales: +1.607.273.7340
Email: sales@CodeSecure.com

Team Support Comes Standard

Software development is a team sport, and we built CodeSonar to fit right in. Findings are persistent and tracked across analyses, even if the location of the code changes in a file. Annotate, rank, assign, search, and compare warnings in the hub or in your issue tracking software. CodeSonar comes with integrations to a variety of commonly used development tools, ensuring a smooth and rapid adoption for your team.



DevSecOps Integration Built-In

Integrating CodeSonar into your software development environment will provide your team with the accurate results they need. CodeSonar works in air-gapped, on-premise, distributed, and cloud-based CI/CD environments for maximum flexibility and scalability. CodeSonar enables the shift to DevSecOps by integrating with the most popular CI tools, such as GitLab, GitHub, Jenkins, and others.

- CodeSonar is highly scalable. It can perform quick scans of a developer's changes, a full scan during an integration build, and anything in between. It can operate in parallel and distributed build environments.
- These capabilities are available in on-premise deployments, including secure environments.
- CodeSecure Cloud is available if you have a geographically dispersed team or a mandate to move workloads into the cloud. You can even supply your own cloud infrastructure and mange CodeSecure Cloud yourself.
- With our Qlik and ArmorCode integrations, managers can monitor and report on the state of their multiple projects.
- Developers can view and remediate security issues and quality defects within their preferred tool, and access more detailed information from the CodeSonar hub with just a couple of mouse clicks.

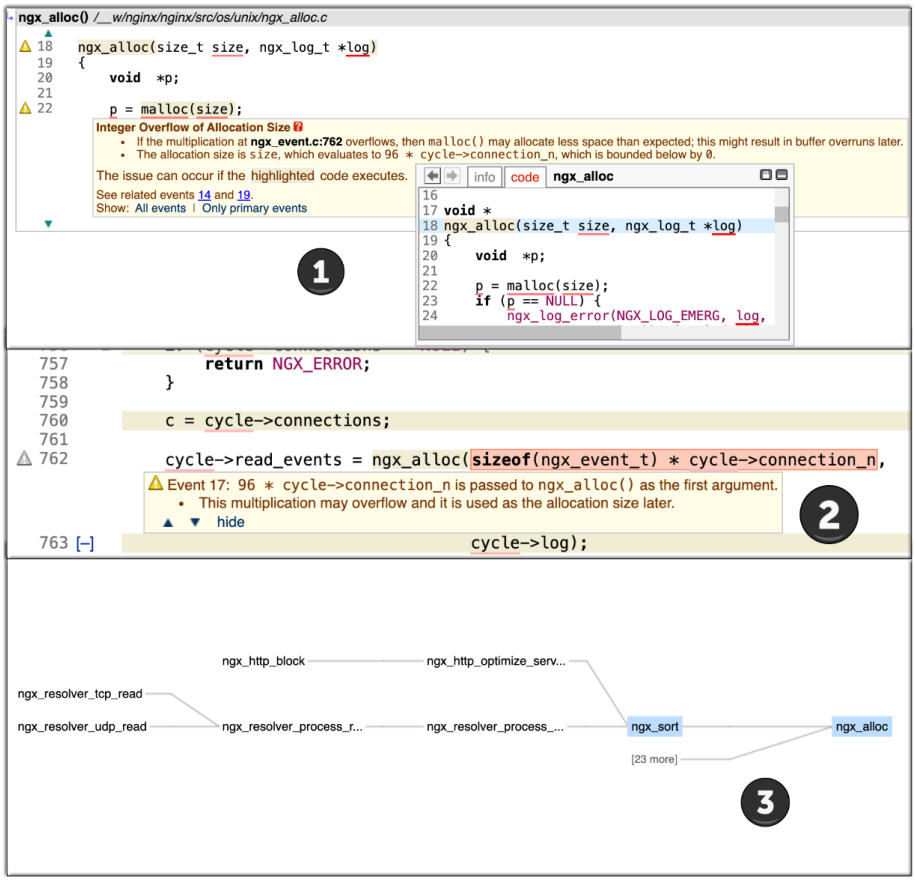
CODESECURE

U.S. Sales: 703.728.8511
International Sales: +1.607.273.7340
Email: sales@CodeSecure.com

Deep Insight

Finding problems is not sufficient. Developers need to understand a problem's root cause and impact in order to address it efficiently. CodeSonar provides comprehensive code browsing capabilities, helping developers understand and fix issues rapidly.

- Analyze the root cause of a warning with information about the complete code path leading to it.
- Assess the risk with a severity score based on the type of warning and the likelihood of the error occurring.
- Help about why a warning ***is*** a warning is just a mouse click away.
- You are in full control with annotations to indicate whether a warning is something you wish to prioritize, suppress, or work on in the future.
- Report on code metrics and quality trends over time to gain insight about project health.
- Visualize the call path and explore interactive charts inside of the CodeSonar hub.
- Export via SARIF, XML, or CSV and analyze your data in third-party applications.



Textual Descriptions
Easy, clear textual descriptions describe what the problem is.

Path Visualization
Shaded background and annotations explain the defect path.

Call Tree Visualization
To understand how a function fits in the larger application.

CODESECURE

U.S. Sales: 703.728.8511
International Sales: +1.607.273.7340
Email: sales@CodeSecure.com

Use Cases

- Software is driving innovation in embedded solutions, including a greater reliance on connectivity for control and monitoring. This has increased the number of threat surfaces, and developers can no longer count on “security through anonymity”. Adding SAST to their development process allows organizations to ensure more reliable and secure operation of their embedded solutions.
- SAST can increase the safety and reliability of enterprises solutions, either built in-house or by a third party. By scanning code as they write it, or by doing binary static analysis on third-party code, organizations can improve quality and increase business continuity.
- Certification can be costly. CodeSonar is certified for ISO 26262, IEC 61508, and EN 50128 projects. It has checkers for all major coding standards to help companies meet the requirements of ISO/SAE 21434, DO 178/330, and many other standards. CodeSonar has powerful reporting features that let you assemble your evidence quickly.

The CodeSecure Difference

- **Deep analysis**. CodeSonar’s advanced analysis engine handles the largest codebases and helps developers pinpoint defects with greater precision.
- **Multi-language support**. Analyze C/C++, Java, C#, Kotlin, Python, GO, Rust, JavaScript, TypeScript, or binaries.
- **Functional safety**. CodeSonar is pre-qualified for the highest levels of safety for the IEC 61508, ISO 26262, and CENELEC EN 50128 standards. Artifacts for qualification according to DO 178C / DO-330 are also available.
- **Flexible deployment**. On-premises, air-gapped, or cloud hosted options are available.
- **Binary analysis**. Analyze legacy applications or third-party binaries.

U.S. Sales: 703.728.8511
International Sales: +1.607.273.7340
Email: sales@CodeSecure.com

CodeSonar C/C++

Compiler Model Support

- ARM Real View
- Clang
- Gnu
- Microsoft
- Freescale CodeWarrior
- IAR
- TASKING
- Green Hills
- Wind River
- QNX
- Keil
- Borland
- Intel
- SHARC, TigerSHARC
- Blackfin
- CodeVision
- MPLAB
- Texas Instruments
- Cosmic
- Hi-Tech

Functional Safety

- Pre-qualified for the highest levels of safety for the IEC 61508, ISO 26262, and CENELEC EN 50128 standards.
- Artifacts for qualification according to DO-178C / DO-330 are also available.

Safety and Security Standards

- **Safety Critical**: MISRA C 2023, MISRA C++, AUTOSAR C++ 14, JSF++
- **Security**: CERT, DISA STIG, OWASP, CWE

CodeSonar Java and C#

Warning Classes

Security

- Buffer overruns
- Injections
- Cryptography
- Cookies
- Passwords
- LDAP

Quality

- Nullness
- Approximation
- Close Resource
- Dead Code
- Bad Eq
- Equals Hash Code

Language Support

- C/C++
- Java
- C#
- Kotlin
- Python
- Go
- Rust
- JavaScript
- TypeScript

IDE Support

- Visual Studio
- Visual Studio Code
- Eclipse

System Requirements

- **Host**: Windows, Linux, FreeBSD, NetBSD.
- **Hardware**: 2+ Cores, 2+ GiB of RAM, 15+ GiB of disk.
- **Compilers**: Supports GCC, clang, Visual Studio, and most embedded compilers.
- **Languages**: C/C++, Java, C#, Kotlin, Python, Go, Rust, JavaScript, TypeScript, and binaries.
- **Output**: SARIF, XML, CSV, PDF, or HTML.

CODESECURE

U.S. Sales: 703.728.8511
International Sales: +1.607.273.7340
Email: sales@CodeSecure.com