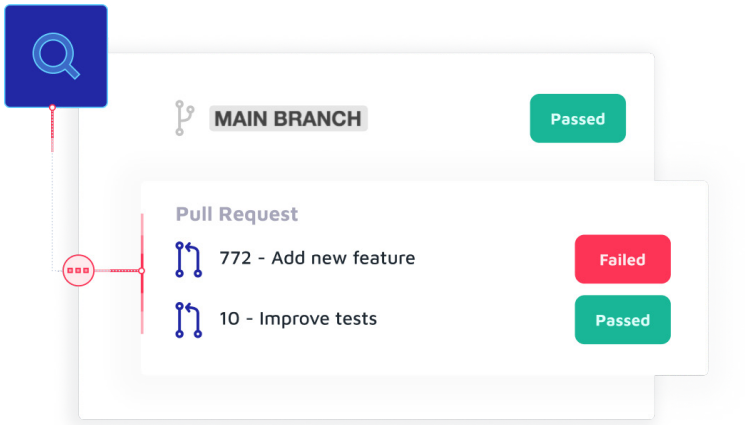
SOLUTION BRIEF

Security starts with Clean Code

Delivering secure code is essential for ensuring the future success of your software, and it requires more than just fixing vulnerabilities. Sonar enables development teams and organizations to apply Clean Code practices and Static Application Security Testing (SAST) to detect all types of issues developers encounter before becoming a security liability.

Clean Code supports secure software development

Sonar's industry-leading Clean Code products offer automated code review and advanced static analysis techniques, such as static taint analysis and symbolic execution. Sonar products are designed to detect and fix a wide range of code quality issues, bugs, and security vulnerabilities for over 30 programming languages and frameworks. From the IDE with SonarLint through the DevSecOps workflow with SonarQube and SonarCloud, developers and security champions can more effectively work together to ensure the security and reliability of their codebase.



Why Clean Code is essential to your security strategy

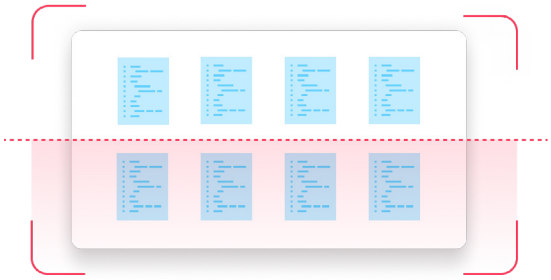
Poorly written, unmaintained code is prone to downtime and attacks. Today, security teams waste time on lengthy feedback loops to the development teams to remediate overlooked issues. Plus, asking developers to context switch and spend cycles to debug and fix issues in the code can be disruptive and frustrating.

It's best to address security issues as code is developed. Sonar provides a multifaceted Clean Code approach to security with a combination of products, education, and methodologies, making delivering secure code fast and easy. With tight integration into the DevSecOps workflow, Sonar products enable developers to detect, understand, and remediate issues as they code. Additionally, the Clean as You Code methodology empowers developers to focus on the quality and security of their current code. This shift left approach of Clean Code highlights that the quality and security of code are intertwined and embeds security as an integral and quickly adopted part of the development process.

With Clean Code from Sonar:

1. Issues are raised as code is developed in the IDE and during the build and commit, where the developer reviews Pull Requests in the DevOps platform before the code is merged.
2. Issues are clearly explained in the context of the code being developed. The developer gets a clear understanding and guidance on why it's an issue and how they can fix it immediately.
3. Issues addressed upfront eliminate the need for extra triaging from the security team. The Clean as You Code approach intrinsically handles this.
4. The analysis is fast and accurate, with fewer false positives. Instead of raising many issues like many tools do, only issues that must be fixed immediately are raised as critical.

Sonar streamlines communication and visibility between development and security teams because issues are addressed early and often. When developers take ownership of fixing security issues in their code as part of their workflow, fewer issues reach audit. This ultimately frees up security teams to focus more on optimizing the performance of the software, applications, and networks.



deeper SAST

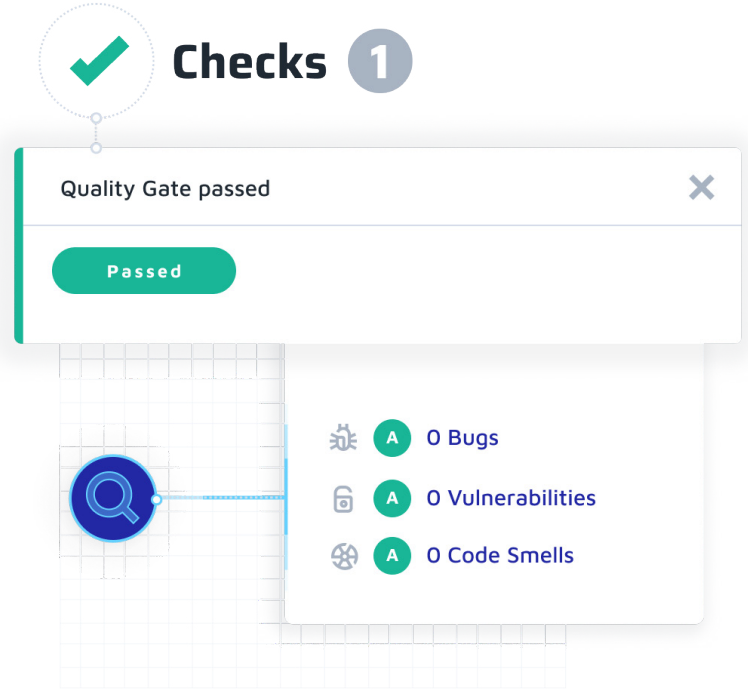
Sonar's deeper SAST empowers organizations to identify and resolve code issues originating from interactions with third-party open-source libraries. This unique capability boosts Sonar's existing SAST engine - which already encompasses deep taint analysis, comprehensive security rules, and cloud secret detection - to trace data flow in and out of libraries. This effectively uncovers deeply concealed security vulnerabilities that other tools fail to detect.

Now, with this innovative technology, organizations can confidently tackle code security challenges, achieve robust application security, and enjoy the benefits of a reliable and fortified codebase.

Available today for Java, C#, and JavaScript/TypeScript, deeper SAST supports thousands of commonly used Open Source libraries, including their subsequent dependencies.

Security-focused features

- **Fine-tuned security analyzers**: Sonar security analyzers are continually improved by our experts and community for precision, accuracy, speed, and coverage – no tuning is required to achieve the acceptable false positive rate. Sonar detects flaws for all code and often exceeds a true positive rate (TPR) of 90%.
- **Embedded advanced SAST capabilities**: deeper SAST is available by default with SonarQube and SonarCloud at no additional cost, runs as part of code analysis, and integrates seamlessly with the CI/CD pipelines. Sonar detects bugs and security flaws at the code level – source code, support code (including config code, infrastructure code, scripting, and test code), and more.
- **Advanced analysis capabilities**: Sonar supports full and detailed analysis of branches and Pull Requests (PRs), providing analysis results in minutes. Built-in, incremental analysis, and server-side caching allow the engine to recognize and analyze only changed files – significantly speeding up subsequent analysis.
- **Extensive Clean Code rules coverage**: Sonar covers over 5,100 rules that detect issues that can lead to vulnerabilities, hotspots, and bugs across 30 programming languages and infrastructure technologies. Security coverage includes all common threats such as cross-site scripting, SQL injection, path injection, secret detection, IaC misconfigurations, phishing, and many others.
- **Security-specific enterprise reporting**: Dedicated reports track the application's code security against standards such as OWASP Top 10, OWASP ASVS, CWE Top 25 (2021, 2020, and 2019), and PCI DSS.



Benefits that matter most

Accelerate secure development:
Utilizing Sonar deeper SAST in the development phase allows developers to find and fix hidden security vulnerabilities and bugs proactively before attackers can exploit them, significantly reducing potential application downtime.

Reduce the risk of security breaches:
Prevent malicious attacks and protect sensitive information with security rules that detect hard-coded credentials and secrets in code. This cloud secret detection uncovers unintended hard-coded passwords, tokens, cloud access keys, API keys, and more in the most popular cloud providers.

Streamline issue remediation:
Improve the overall security posture of your software with automatic analysis and reduce reliance on manual code reviews. Developers can focus on quick and effective remediation, saving time and money.

Ensure code security and compliance:
Track code security compliance and evaluate the risks on software assets at an enterprise level with detailed reports. Security reports, executive aggregation, and PDF reports provide the oversight larger organizations need to evaluate risks on their software assets.

Real-time feedback and education:
Sonar meets developers where they're working with in-product, contextual Clean Code education that identifies issues, explains why the issue occurred, and presents remediation guidance. Developers gain immediate and insightful remediation advice from the IDE with SonarLint to the code review cycle with SonarQube and SonarCloud.

Industry-best security standards

Sonar adheres to OWASP's industry-recommended practices and holds an ISO 27001 certificate at the company level. Sonar also has IronBank-accepted processes for software vulnerability management, dependency scanning, and quality. Sonar products, user interfaces, APIs, and authentication mechanisms regularly pass penetration testing conducted by external cyber and application security companies. The company runs these at a minimum of twice per year.

Sonar encourages researchers and members of its community that find vulnerabilities to submit and report them to the security team. Sonar has a dedicated internal team of security researchers that regularly evaluates product security, and reports discovered bugs and vulnerabilities following public disclosure principles.

Secure code enables secure software

Clean Code from Sonar empowers developers to produce high-quality, sustainable, and innovative software while putting security teams in a position to focus on software parts that require deep manual audits. Sonar's forward-leaning vision encompasses the needs of environments such as cloud-native apps and cloud/hybrid deployments, anticipating the need for zero-compromise testing to tackle the potential impacts of poor-quality code. Developers and security teams must operate at the code level for organizations to get the most value out of their software.

Sonar is the home of Clean Code, trusted by more than 7 million developers and more than 400 thousand organizations worldwide.

VISIT SONARSOURCE.COM - - ->