Beyond first-party code

Securing the software supply chain with SonarQube Advanced Security

With SonarQube, you've already made an investment in code quality and code security. Your teams benefit from core capabilities essential for securing the code they write. And all of it is delivered by starting left in the developer's workflow- in their integrated development environments (IDEs), in pull requests (PRs), in continuous integration (CI).

The risk: Dependencies & supply chain

But the way you build software has changed. Modern applications are no longer just the code in your repositories. They are heavily composed of frameworks, open-source libraries, SDKs, APIs, and transitive dependencies pulled in automatically. Your attack surface has shifted from just "your code" to the entire software supply chain that code depends on. These introduce key risks that need to be addressed:

1 Vulnerable dependencies:

Critical vulnerabilities often live in libraries and frameworks—code that isn't written by your team. A normal Static Application Security Testing (SAST) engine that only analyzes your first-party code won't see these risks. Your code looks "secure," but the version of a dependency you rely on may be exploitable.

2 License policy violations:

It's easy to pull in libraries without fully understanding their licenses, creating legal and compliance problems. Without visibility, you can't confidently answer: "What are we using, and are we allowed to use it this way?".

3 Dangerous interactions between your code and dependencies:

Some issues only appear when your code calls certain APIs or uses libraries with insecure patterns or defaults. Traditional SAST ignores dependency behaviors and can miss real-world vulnerabilities at this boundary.

4 Malicious packages:

Malicious packages in third-party dependencies introduce hidden vulnerabilities into your software supply chain. These compromised libraries can lead to data breaches, system disruptions, and unauthorized access.

SonarQube Advanced Security

SonarQube Advanced Security is available for SonarQube Enterprise and higher, enhancing your security posture to now include your entire software supply chain. It extends your protection in two critical ways:

Software Composition Analysis (SCA)

SCA manages risks within your open source software supply chain:

- Detects vulnerabilities in both direct and transitive dependencies.
- Automatically identifies the licenses of all dependencies and helps ensure they comply with your organization's policies, simplifying complex legal compliance.
- Generates SBOMs (Software Bills of Materials) in standard formats like CycloneDX and SPDX for transparency, security audits, and compliance requirements.
- Detects malicious packages and potential malware within your dependencies.

Advanced SAST (First-party code + dependency interactions)

Advanced SAST applies Sonar's taint analysis to focus on the interaction between your code and open source dependencies:

- Extends taint analysis to trace data flows in and out of third-party library code.
- Finds deeply hidden, complex vulnerabilities that arise from how your code uses specific open source libraries and frameworks that traditional SAST tools miss.

This doesn't replace your existing setup; it extends the same developer-first UX and CI/CD pipeline integration, now with end-to-end visibility in one place. SonarQube Advanced Security helps your teams transition from "we secure the code you write " to "we secure all the code in your applications".

Technical use cases:

Technical use case	Why it matters	SonarQube benefits
Third-party vulnerability detection and management	You are responsible for the security of your entire application, and over 80% of the code of modern applications is open-source libraries that can introduce known vulnerabilities (CVEs) or subtle, hard-to-find flaws.	SonarQube Advanced Security includes SCA to flag known vulnerabilities in your direct and transitive dependencies.
Open source license compliance	You need to confirm that third-party code licenses comply with your organization's legal policies without manual review.	SonarQube Advanced Security's SCA automatically identifies licenses of all open-source dependencies and flags compliance risks, simplifying the complex legal overhead
SBOM generation	You need an automatic, detailed inventory of your application's components to meet compliance requirements and simplify rapid vulnerability response.	SonarQube Advanced Security automatically generates a SBOM in industry-standard formats like CycloneDX and SPDX, providing essential transparency for audits and compliance.
Dependency-aware injection flaws	You need to go beyond first-party code and discover how your code interacts with the third-party dependencies.	Advanced SAST helps uncover deeply hidden injection flaws which might occur when your first-party code interacts with third-party libraries used in your code.