Datasheet

Developer-first SCA across your workflow with SonarQube

Reduce software supply chain risk without sacrificing velocity

SonarQube Advanced Security includes software composition analysis (SCA), which helps you secure and govern open source dependencies without slowing developers down. It delivers dependency risk intelligence across IDE, pull requests, and CI/CD, combining CVE detection, license management, malicious package detection, and SBOM visibility in a single, integrated workflow.

The cost of unmanaged dependency risk

- **Hidden risks:** Vulnerabilities often hide deep and transitive dependency trees, making it difficult to understand their true impact or prioritize remediation effectively.
- **Release bottleneck:** Alert fatigue and manual reviews slow delivery, especially when security and licensing decisions arrive too late in the development cycle.
- **Evolving supply chain threats:** Modern threats now include malicious packages (e.g., typosquatting, dependency confusion) that can enter builds through standard dependency management, often without a traditional CVE signal.

SonarQube Key Capabilities

- **Detect vulnerable dependencies (CVE detection):** Identify and surface vulnerabilities (CVEs) within direct and transitive dependencies as a native part of your analysis workflow.
- **License management:** Flag license risks early with policy-based checks to avoid legal issues during the release phase.
- **SBOM visibility:** Automatically produce a SBOM in standard formats to provide visibility needed for audits and supply-chain governance.
- **Detect malicious packages in CI/CD:** Detect publicly known malicious packages and raise high-priority risk signals the moment they are pulled into your builds.
- **Continuous monitoring:** Regularly re-analyze your codebase to surface newly disclosed dependency risks and ensure your quality gates remain current.
- **Supported languages:** Supports a wide range of languages including Javascript, Typescript, Python, C# and many more providing industry-leading dependency analysis across your portfolio.

Benefit	What you get with SonarQube Advanced Security
Integrated dependency security	CVE detection, license management, and SBOM visibility, and malicious package detection delivered in one unified developer workflow.
Prevention-first pipeline guardrails	Catch risky dependency changes early and enforce policies through quality gates before they reach main or release branches.
Reduced tool sprawl	Consolidate your code quality and security analysis including software supply chain to simplify operations and improve developer experience.
Dependency-aware data flow analysis	Traces untrusted data as it flows into and out of third-party open source libraries, enabling detection of deeply hidden complex injection vulnerabilities.