Fortify's Software Composition Analysis, powered by Sonatype, helps you manage your open source and third-party risk and vulnerabilities to secure your software supply chain.

1. Integrated platform
   Fortify combines static analysis (SAST) and software composition analysis (SCA) into a single platform. The integrated results from Sonatype’s Nexus Lifecycle, alongside findings from Fortify Static Code Analyzer (SCA), provides a consolidated view of application vulnerabilities.

2. Complete bill of materials
   Scans binaries to identify open source components and creates a software bill of materials, with remediation tips that include the next known vulnerability version.

3. Largest database of public and private vulnerabilities
   Sonatype uses artificial intelligence and machine learning, along with human curation to ingest and identify security vulnerabilities, to detect 70% more vulnerabilities than the NVD database alone.

4. Susceptibility analysis
   Reduces known vulnerability false positives, eliminates effort of needlessly upgrading libraries, and saves time on investigating known issues in open source (tech preview for on premises/Java only).

5. Build into CI/CD
   Scan anytime in your pipelines, configure to work with your process.

Learn more about Fortify’s Software Composition Analysis with Sonatype.

Watch the video
Visit Software Composition Analysis page