

# Snyk vs SonarQube

A vendor-neutral technical comparison for security teams | March 2026



[konvu.com/compare/snyk-vs-sonarqube](https://konvu.com/compare/snyk-vs-sonarqube)

**TL;DR** Snyk is the stronger SCA platform and unified security tool. SonarQube is the stronger code quality enforcer with mature SAST. Snyk leads on developer experience and supply chain security. SonarQube leads on quality gates, pricing at scale, and self-hosted deployment. Most teams run both.

## Head-to-head overview

Category	Snyk	SonarQube
Origin	SCA-first (2015), added SAST via DeepCode acquisition (2020)	Code quality-first (2007), added SCA in 2025 (Enterprise add-on)
SAST approach	AI/ML-based data flow (opaque rules, no practical custom rule writing)	AST pattern matching + taint analysis (transparent rules, fully customizable)
SCA approach	Proprietary vuln DB, ~18 ecosystems, CVE Numbering Authority, reachability	Enterprise add-on only (2025), ~8 ecosystems, no reachability analysis
Custom rules	Early Access, Enterprise-only, proprietary Datalog query language	Mature: Java API, XPath, Quality Profiles, 6,500+ built-in rules
Scan speed	No build step required. Reported as 10-50x faster for SAST	Requires build. Slow for large projects. Single queue on Community
Enterprise	FedRAMP, custom RBAC (Enterprise), multi-region data residency, SaaS	Self-hosted (full data control), compliance reporting (OWASP, CWE, PCI DSS)

## What independent benchmarks show

Source	Metric	Snyk	SonarQube
EASE 2024 (ACM)	Detection rate (default config)	11.2% (lowest of 4 tools)	Not tested
Lenarduzzi 2021 (Springer)	True positive rate (all warnings)	No academic data	18% (82% FP rate)
OWASP Benchmark	Java plugin score	Not tested	33.34% (older Community version)
G2 reviews	Overall / FP score	4.5/5 overall, FP score: 6.8/10	4.4/5 overall
Gartner Peer Insights	Reviews / Rating	202+ reviews, 4.4/5, 3x Customers' Choice	Fewer reviews

## Pricing at a glance

Company size	Snyk (estimated)	SonarQube (estimated)
Startup (<20 devs)	Free (limited) or ~\$3K-\$6K/yr Team	Community Build free; Developer ~\$720-\$2K/yr
Mid-market (50 devs, 2M LOC)	~\$63K/yr (Ignite at \$1,260/dev/yr), SSO requires Ignite	Developer ~\$10K/yr; Enterprise ~\$20-35K/yr, Unlimited users
Enterprise (200+ devs)	\$135K-\$500K+/yr (custom), FedRAMP available	Enterprise ~\$40-70K/yr + Advanced Security add-on, Self-hosted

## When to pick which

### Pick SonarQube when:

- Code quality enforcement matters (quality gates, coverage, duplication)
- Self-hosted deployment is required (full data control)
- Budget is constrained at scale (LOC pricing, unlimited users)
- Legacy language support needed (COBOL, ABAP, PL/SQL)

### Pick Snyk when:

- SCA is the primary need (best-in-class, Forrester Leader)
- Unified security platform wanted (SCA+SAST+IaC+Container+DAST)
- Cloud-native architecture (container + IaC scanning)
- FedRAMP compliance is required

Sources: EASE 2024 (ACM), Lenarduzzi et al. 2021 (Springer), OWASP Benchmark, G2, Gartner Peer Insights, Vendr. Full article:

The bottleneck is rarely detection. It's triage. If triage is still the problem, that's what Konvu solves.

[konvu.com/compare/snyk-vs-sonarqube](https://konvu.com/compare/snyk-vs-sonarqube)

[konvu.com/demo](https://konvu.com/demo)