Semgrep vs SonarQube

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

konvu

konvu.com/compare/semgrep-vs-sonarqube

TL;DR Semgrep is the stronger security scanner with best-in-class custom rules and SCA reachability. SonarQube is the stronger code quality enforcer with mature quality gates and self-hosted deployment. They are complementary. Most teams that need both security and quality run both.

Head-to-head overview

Category	Semgrep	SonarQube
Origin	Security-first SAST (2020), added SCA (2022) and Secrets	Code quality-first (2007), added SCA in 2025 (Enterprise add-on)
SAST approach	Pattern matching + taint analysis (YAML rules, transparent, highly extensible)	AST pattern matching + taint analysis (Dev Edition+, transparent, customizable via Java)
SCA approach	Supply Chain: 14 languages, 15+ pkg managers, reachability analysis	Advanced Security add-on: ~5 ecosystems, no reachability, Enterprise-only
Custom rules	YAML rules using target language syntax. 20K+ Pro rules, 2.4K+ community rules	Java plugin API (steep), XPath (limited languages), 6,500+ built-in rules
Scan speed	Fast: ~10s diff-aware PR scans. SaaS-first, no infrastructure needed	Slower: client-server architecture adds latency. Single queue on Community
Enterprise	SaaS-first, SSO (Team+), limited RBAC, no FedRAMP, Managed Scans	Self-hosted (full data control), compliance reporting (OWASP, CWE, STIG, PCI DSS)

What independent benchmarks show

Source	Metric	Semgrep	SonarQube
EASE 2024 (ACM)	Detection rate (default config)	CE: 14.3%. Custom rules: 44.7%	Not tested
DryRun Security 2025	Seeded vuln detection (default)	46% (12/26)	19% (5/26)
Doyensec 2025	CE vs Pro true positives	CE: 44-48%, Pro: 72-75%	Not tested
Lenarduzzi 2021 (Springer)	True positive rate (all warnings)	No academic data	18% (82% FP rate, all warning types)
G2 / Gartner	Reviews and ratings	G2: 4.7/5. Gartner MQ 2025 (Niche Player)	G2: 4.4/5. Forrester Wave SAST Q3 2025

Pricing at a glance

Company size	Semgrep (estimated)	SonarQube (estimated)
Startup (<20 devs)	Free tier: Pro engine, all rules, SCA, Secrets (10 contributors)	Community Build free (no taint, no branches); Developer ~$720-$2.5K/yr
Mid-market (20-200 devs)	~$8.4K-$84K/yr (Team at $35/contributor/mo per product)	Developer ~$2.5-10K/yr; Enterprise ~$20-35K/yr. Unlimited users
Enterprise (200+ devs)	$50K-$193K+/yr (custom). Per-contributor pricing scales with team	Enterprise ~$20-70K/yr + infra costs. LOC-based: cheaper at scale

When to pick which

Pick Semgrep when:

- Security scanning is the primary driver (2.4x more detections vs SQ)
- Custom rules matter (YAML rules, 20K+ registry, write in minutes)
- SCA with reachability needed (14 languages, ~98% noise reduction)
- Small team on a budget (free tier includes Pro engine for 10 devs)

Pick SonarQube when:

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

Sources: EASE 2024 (ACM), DryRun Security 2025, Doyensec 2025, Lenarduzzi et al. 2021 (Springer), G2, Gartner Peer Insights, Vendor documentation

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