Semgrep vs CodeQL

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

konvu

konvu.com/compare/semgrep-vs-codeql

TL;DR Both cost $30/committer/month. CodeQL achieves higher benchmark scores (OWASP F1: 74.4% vs 69.4%) and deeper semantic analysis. Semgrep is faster, easier to extend with custom rules, and CI-agnostic. Many teams run both: Semgrep in CI for fast PR feedback, CodeQL in nightly builds for deeper analysis.

Head-to-head overview

Category	Semgrep	CodeQL
Origin	Security-first SAST (r2c, 2020), added SCA (2022) and Secrets	Semantic analysis engine (Semmle/Oxford, 2006), acquired by GitHub 2019
SAST approach	AST pattern matching + taint analysis (YAML rules, fast, highly extensible)	Whole-program database + QL queries (deep semantic analysis, higher precision)
Custom rules	YAML using target language syntax. Minutes to write. 2.8K+ community rules	QL language (Datalog-derived). Hours to days to learn. 430+ security queries
Scan speed	Fast: ~10s diff-aware PR scans, ~150MB memory, SaaS-first	Slower: minutes to 30+ min, ~450MB memory, database creation overhead
SCA	Supply Chain: 14 languages, reachability analysis, noise reduction	No native SCA. Dependabot via GHAS (no reachability analysis)
Enterprise	SaaS-first, SSO (Team+), CI-agnostic, Managed Scans, no FedRAMP	GitHub-native, FedRAMP authorized, SCIM, audit log streaming, SIEM connectors

What independent benchmarks show

Source	Metric	Semgrep	CodeQL
OWASP Benchmark (arXiv 2025)	F1 Score / Accuracy	F1: 69.4%, Accuracy: 58.9%, FPR: 74.8%	F1: 74.4%, Accuracy: 65.5%, FPR: 68.2%
EASE 2024 (ACM)	Real-world Java vuln detection	Baseline: 11-26%. Custom rules: 44.7% (181% improvement)	Not individually reported (4-tool combo: 38.8%)
Doyensec 2022	OWASP Benchmark (Java)	Better on average; CE limited to single-function analysis	Outperformed in individual CWE categories; 3 CWEs at zero detection
G2 / Gartner	Reviews and analyst ratings	G2: 4.7/5. Gartner MQ 2025 (Niche Player)	Part of GHAS. G2: 4.5/5 (GitHub). Gartner MQ via GitHub

Pricing at a glance

Company size	Semgrep (estimated)	CodeQL / GHAS (estimated)
Startup (<15 devs)	Free tier: Pro engine, all rules, SCA, Secrets (10 contributors, 50 repos)	Code Security: $30/committer/mo ($450/mo for 15 devs) + GitHub plan
Mid-market (100 devs)	~$7,500/mo list (Code $30 + SCA $30/contributor); ~$46.8K/yr negotiated	Code Security: $3,000/mo ($36K/yr); + Secret Protection: $4,900/mo ($58.8K/yr)
Enterprise (500 devs)	$150K-$300K/yr custom (per-contributor pricing scales with team)	$294K/yr list (Code + Secrets). Free for all public repositories

When to pick which

Pick Semgrep when:

- Fast PR feedback needed (10s diff-aware scans vs minutes for CodeQL)
- Custom rules matter (YAML rules written in minutes, 2.8K+ registry)
- CI-agnostic required (first-class GitLab, Bitbucket, Azure DevOps support)
- SCA with reachability needed (Semgrep Supply Chain, 14 languages)

Pick CodeQL when:

- Deep semantic analysis needed (whole-program database, F1: 74.4%)
- GitHub-native workflow (one-click setup, Copilot Autofix, Security Overview)
- Free for public repos (full semantic analysis, no license cost)
- Complex multi-step vulnerability detection (QL query depth advantage)

Sources: OWASP Benchmark (arXiv 2025), EASE 2024 (ACM), Doyensec 2025, G2, Gartner. Full article: konvu.com/compare/semgrep-vs-codeql

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