Snyk vs Semgrep

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

konvu

konvu.com/compare/snyk-vs-semgrep

TL;DR Snyk is the stronger SCA platform. Semgrep is the stronger SAST engine. Snyk leads on enterprise features and compliance. Semgrep leads on rule customization, speed, and pricing. Neither covers everything alone.

Head-to-head overview

Category	Snyk	Semgrep
Origin	SCA-first (2015), added SAST via DeepCode acquisition (2020)	SAST-first (open-source, ex-Meta), added SCA as Supply Chain
SAST approach	AI/ML-based data flow (opaque rules, no practical custom rule writing)	AST pattern matching + taint tracking (transparent YAML rules, fully customizable)
SCA approach	Proprietary vuln DB, ~18 ecosystems, CVE Numbering Authority	Lockfile parsing + reachability analysis, 14 languages, 12 with reachability
Custom rules	Early Access, Enterprise-only, proprietary Datalog query language	First-class feature, all tiers. YAML syntax using target language
Scan speed	Cloud-based, adds network latency. Reported as slower in benchmarks	Local execution, completes in seconds on PR scans (G2, Trail of Bits)
Enterprise	FedRAMP, custom RBAC, multi-region data residency, 202+ Gartner reviews	3 fixed RBAC roles, US data residency default, no FedRAMP, 14 Gartner reviews

What independent benchmarks show

Benchmark	Metric	Snyk	Semgrep
EASE 2024 (ACM) 170 real Java vulns	Detection rate (default config)	11.2% (lowest of 4 tools)	14.3% (CE, no Pro)
Doyensec (OWASP apps)	True positive rate (CE vs Pro)	Not tested	CE: 44-48% Pro: 72-75%
G2 reviews	Overall / FP score	4.5/5 overall FP score: 6.8/10	4.7/5 overall "minimal false positives"
Forrester Wave Q4 2024 SCA	Market position	Leader, "Customer Favorite"	Not included in evaluation

Pricing at a glance

Company size	Snyk (estimated)	Semgrep (estimated)
Startup (<20 devs)	Free (limited) or ~$3K-$6K/yr Team	Free tier: full Pro engine for <=10 contributors
Mid-market (20-200)	~$25K-$135K/yr (Ignite tier) SSO requires Ignite ($1,260/yr/dev)	~$8.4K-$84K/yr (Team at $35/contributor/mo) SSO included in Team tier
Enterprise (200+)	$250K-$500K+/yr (custom) FedRAMP available	Custom pricing No FedRAMP

When to pick which

Pick Semgrep when:

- Programmable detection is a priority
- Budget matters (generous free tier)
- SAST is the primary need
- Scan speed is critical (local, seconds)

Pick Snyk when:

- SCA is the primary need (best-in-class)
- Unified platform wanted (SCA+SAST+IaC+DAST)
- Compliance reqs are strict (FedRAMP, RBAC)
- No AppSec team (works out of the box)

Sources: EASE 2024 (ACM), Doyensec, G2, Gartner Peer Insights, Forrester Wave Q4 2024, Vendr. Full article: konvu.com/compare/snyk-vs-semgrep

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

konvu.com/demo