Semgrep

Built for builders, trusted by security: Reduce AppSec noise, catch, flag and fix real issues before they ship

Today's IT and security leaders are under siege. Legacy AppSec tools generate mountains of false positives, misalign security teams from developers, and fail to catch the logic and authorization flaws that attackers exploit most. Budgets are constrained, developer velocity is non-negotiable, and scaling security across cloud-native environments has never been more complex. Meanwhile, every undetected vulnerability that ships is a liability waiting to surface.

What if you could eliminate the noise, align security with development, and catch vulnerabilities that actually matter without sacrificing speed?

You can't solve a modern security problem with yesterday's tools

For the security practitioner

Legacy AppSec tools flood teams with inaccurate alerts and miss the vulnerabilities that matter most. Semgrep combines deterministic static analysis with AI reasoning to uncover real vulnerabilities, prioritize reachable risks, and dramatically reduce false positives.

For the developer

Security tools that interrupt workflows and cry wolf with false positives kill productivity. Semgrep lives where developers work and fits directly into existing IDEs and CI/PR pipelines, delivering fast, trustworthy feedback that helps developers ship secure code without breaking flow.

What high-performance AppSec looks like in practice

95% of security reviewers validated AI-learned context that cuts false positives and prioritizes reachable vulnerabilities, across 6M+ findings.

95%

80% fewer false positives AppSec teams triage across code and supply chain, dramatically shrinking the backlog.

80%

16% better false-positive detection with Semgrep + Anthropic's Claude on Amazon Bedrock—less noise, less triage.

16%

To date, Semgrep has delivered at scale for modern development teams:

43M+
pull request scans

75M+
total scans

36B+
lines of code analyzed

> "Semgrep lets us treat security and code quality as first-class priorities. The combination of customizable CI/CD configurations, custom rules, and finding policies gives us a SAST program that actually fits our codebase.
>
> –**Zach Rayburn**, Staff Product Security Engineer, Cribl

Read more

About Semgrep

Trusted by innovative companies like Figma, Dropbox, Slack, and Lyft, Semgrep is a leading global application security platform purpose-built for modern development teams and the leader in code security for builders.

Engaged with the Amazon Web Services (AWS) Global Startup Program and available in AWS Marketplace, Semgrep helps AWS-native teams reduce AppSec noise while improving coverage of the vulnerabilities that matter most. Unlike legacy static application security testing (SAST) tools that flood teams with alerts and miss what matters, Semgrep combines deterministic static analysis with AI-powered detection to catch high-impact vulnerabilities, including logic and authorization flaws, earlier in the development lifecycle. The result is high-signal security that fits seamlessly into existing workflows, giving security leaders provable ROI and developers the fast, friction-free feedback they need to ship with confidence.

Learn more at semgrep.dev

Semgrep

aws PARTNER