CUSTOMER SUCCESS STORY

Shipping secure code to AWS at engineering speed

How Sola Security scans every pull request and its infrastructure-as-code before anything reaches AWS

Overview

Sola Security is an AI platform that lets security teams rapidly build and deploy tools across their stack using natural language prompts.

As its own security organization matured, Sola made a deliberate decision to raise the bar on secure coding without slowing developers down. The goal was high-quality, scalable security automation that fits naturally into how developers work, not simply another tool in the stack.

Sola's code lives in GitHub, and Semgrep runs as part of its GitHub Actions pipelines. Those pipelines deploy a wide range of AWS services, including Amazon S3, Amazon RDS, Amazon ECS, Amazon EKS, AWS Lambda, Amazon CloudFront, and Amazon API Gateway.

Because Sola defines its infrastructure in Terraform, Semgrep scans both application code and infrastructure-as-code before anything is deployed to AWS. AWS provides the secure, scalable foundation, and Semgrep secures the code and configuration built on top of it.

The challenge: Scaling security without friction

Sola needed security that could scale with engineering velocity without relying on manual review or tribal knowledge. The team works in a large monorepo, so the tool had to stay stable at that scale and still produce high-quality findings.

The evaluation focused on **speed**, so scans wouldn't slow CI pipelines; **stability**, so it could run on every pull request; and **depth**, with dataflow analysis between sources and sinks, including across files.

The team also wanted AI that analyzes findings and learns from past triage decisions through memory, plus the ability to write custom rules for its own environment.

After a hands-on evaluation of multiple AppSec tools, Sola selected **Semgrep Code**, **Semgrep Supply Chain**, and **Semgrep Secrets**. The Pro engine's interfile, source-to-sink analysis delivered findings the team could trust in a production CI/CD pipeline, where single-file open-source tools lacked context.

Making security transparent to developers

Sola made Semgrep "transparent" to developers. They only encounter it when it finds something important enough to block a pull request.

When that happens, the Semgrep comment in the PR explains exactly what the issue is and why it failed, so developers don't have to change how they work or become security experts.

> "The goal was not to 'add another tool,' but to implement high-quality, scalable security automation that fits naturally into how developers work."
>
> **Yoni Weintrob**
> CISO at Sola Security

© Semgrep 2026

Semgrep

CUSTOMER SUCCESS STORY

Catching issues earlier

As soon as Sola connected Semgrep, it uncovered several important SQL injection issues in the source code.

Semgrep has also made responding to new CVEs much faster. When one is published, the team checks its SBOM and sees in about a minute whether it's running an affected version.

In Sola's DevOps infrastructure repos, Semgrep identified **Amazon API Gateway endpoints that were publicly exposed** and could have been abused to disrupt the application.

Triage was fast because the finding was high-confidence and the team understood exactly how it could be exploited. Remediation was just as quick.

Know your entire infrastructure

Because Semgrep scans Terraform as well as application code, misconfigurations like exposed API Gateway endpoints are caught in the pull request, before they reach production on AWS.

With Semgrep Registry rules enabled for every AWS service it deploys, Sola covers its whole AWS footprint, not just its application code.

> "Know your entire infrastructure. I went through the Semgrep Registry and enabled rules for every AWS service we use, including API Gateway. The very next scan surfaced issues we wouldn't have found otherwise."
>
> **Sola Security**
> Advice for other AWS customers

Measurable outcomes: Security that scales

Coverage: Before the full rollout, Semgrep scanned about 15% of pull requests. Sola's target was 100%, and today 100% of PRs in its monorepo and DevOps infrastructure repos are scanned automatically before deployment to AWS.

Scale: Sola's 2-person security team supported engineering as it doubled from 10 to 20 developers, doubling the developer-to-security ratio from 5:1 to 10:1.

Remediation: High-confidence findings mean Sola triages and fixes issues quickly, and checking exposure to a new CVE now takes about 1 minute.

15% to 100%

of pull requests scanned automatically before deployment to AWS, meeting Sola's 100% target

10:1

developers per security engineer, up from 5:1, as a 2-person team supported 2x engineering growth

About Semgrep

Semgrep enables teams to use industry-leading AI-assisted static application security testing (SAST), supply chain dependency scanning (SCA), and secrets detection. The Semgrep AppSec Platform is built for teams that struggle with noise by helping development teams apply secure coding practices.

© Semgrep 2026