Semgrep aws

CUSTOMER SUCCESS STORY

How Docplanner centralized application security across 400 contributors

Docplanner

By moving from uneven static analysis coverage to a centralized, low-noise approach, Docplanner quickly expanded security coverage across key PHP projects while giving its AppSec team greater control over rules, policies, and developer-facing findings.

CUSTOMER	Docplanner	INDUSTRY	Healthcare technology
ENGINEERING ORGANIZATION	Approximately 400 code contributors	APPSEC TEAM	4 engineers
USE CASE	Static application security testing and developer security workflows	SOLUTION	Semgrep Code with managed scans, custom rules, and AI-assisted triage
AWS SERVICES	AWS WAF and Amazon S3		

Impact

<1 hour

of hands-on time to deploy Semgrep across targeted repositories representing approximately 30% of production services

~30%

reduction in rule-based findings through AI-assisted triage over three months

4–6 hrs

of manual triage effort avoided per week (estimated equivalent, based on alerts provisionally ignored)

- Centralized static analysis for key PHP projects and selected repositories.
- Gave AppSec direct control over rules, policies, enforcement modes, and scan configurations.
- Turned vulnerabilities discovered during assessments into reusable rules for detecting variants.
- Integrated Semgrep findings into Docplanner's existing reporting and security assessment workflows through APIs.

Overview

Docplanner is a healthcare technology company that helps patients find healthcare professionals and book appointments online. It also provides software that supports healthcare providers in managing their practices and patient interactions. Protecting that environment requires application security that can scale. Docplanner's four-person AppSec team supports approximately 400 code contributors across a distributed organization. It works alongside SecOps, platform security, and the broader platform organization, combining direct collaboration with developers and automation to identify new repositories and apply security measures based on project context.

Docplanner does not rely on a formal security champions program. Engineering teams can be reshaped as product and market priorities change, making a fixed champion structure difficult to maintain. Instead, AppSec maintains relationships with security-minded developers, provides clear channels for questions and reporting suspicious activity, and uses automation to bring security controls into new repositories.

Operating in healthcare adds another layer of responsibility. The team prioritizes coverage for high-value applications, including systems that handle user and healthcare information.

> "Because we are in healthcare, we also have certifications that require us to pay close attention to security."
>
> **Agnieszka Pietruczuk**
> AppSec Team Lead, Docplanner

© Semgrep 2026

Protecting healthcare applications with a layered security approach

Docplanner combines cloud-based security controls with proactive application security throughout the development lifecycle. As documented in an AWS-published customer case study, Docplanner uses AWS WAF to protect its web applications from malicious traffic and distributed denial-of-service attacks. The company also exports AWS WAF logs to Amazon S3 to support security analysis and the development of additional protection rules.

Complementing these AWS capabilities, Docplanner uses Semgrep to identify vulnerabilities in application source code, implement custom security rules, and prioritize findings through AI-assisted triage. This approach combines cloud-based traffic protection, security analysis, and developer-focused application security as part of Docplanner's broader security program.

The challenge: Scaling coverage without creating more noise

Before Semgrep, static analysis existed in different parts of Docplanner's environment, but coverage and implementation quality varied by repository. The AppSec team wanted a more systematic approach to static analysis across its highest-priority projects. The team also wanted to avoid a common AppSec problem: increasing coverage while overwhelming developers with findings.

Low-noise results were a requirement from the beginning. For Docplanner, success meant establishing a dependable security baseline across high-priority applications rather than maximizing the raw number of findings.

> "Reducing false positives and noise for developers was one of the main requirements for whatever tools or approaches we used."
>
> **Andrii Kudiurov**
> Senior AppSec Engineer, Docplanner

The solution: The right balance of speed, flexibility, and control

Docplanner uses Semgrep as part of a broader application security toolset. The team needed a semantic analysis engine with strong PHP support, fast execution, flexible custom rules, and a straightforward way to onboard projects.

Managed scans enabled Docplanner to expand coverage quickly, while the Semgrep platform gave AppSec control over rules, policies, and how findings were presented to developers. Semgrep also gave Docplanner flexibility without requiring the team to build and maintain another layer of integration.

> "We needed a semantic engine, and we needed it for PHP. The speed of execution is useful, the custom rules are useful, AI triage helps, and managed scans let us onboard a project quickly."
>
> **Andrii Kudiurov**
> Senior AppSec Engineer, Docplanner

© Semgrep 2026

From scattered analysis to centralized control

Managed scans helped Docplanner quickly deploy Semgrep across selected projects. Rolling out Semgrep to targeted repositories representing approximately 30% of production services required less than one hour of hands-on time. Once coverage was in place, the AppSec team could add rules, change policies, adjust enforcement, and update scan behavior through the platform.

That flexibility matters in an environment where repositories do not all follow the same branch strategy. Within the scope Docplanner defined for Semgrep, the rollout delivered the coverage and developer collaboration the team expected.

> "When it comes to speed of integration, ease of deployment, and ease of management, the experience was very streamlined. If tomorrow I want to scan another branch in five projects, I can do it through the cloud console. I don't have to write extra automation. I change it, and it works."
>
> **Andrii Kudiurov**
> Senior AppSec Engineer, Docplanner

High-signal findings without overwhelming developers

Docplanner's deployment strategy begins with the quality of its rules. The AppSec team selects high-signal rules for active enforcement and can configure them to comment on code or block a change. Other findings remain available for security review without interrupting the developer workflow. That separation gives AppSec time to tune a rule before making it part of the developer workflow. Semgrep's AI-assisted triage helps the team review additional findings, separate likely signal from noise, and understand which rules perform well.

Over a three-month period, Docplanner reported that AI-assisted triage reduced rule-based findings by approximately 30%. Based on the volume of alerts provisionally ignored, Docplanner estimates an equivalent of approximately 4–6 hours of manual triage effort avoided per week, rather than directly measured staff time savings.

> "We started triage with the rules rather than the findings. We select high-signal rules that can interrupt developers, and keep the other findings in the background so we can see what is happening without creating noise."
>
> **Andrii Kudiurov**
> Senior AppSec Engineer, Docplanner

© Semgrep 2026

Turning vulnerabilities into reusable security rules

Custom rules give Docplanner a way to turn an individual discovery into a repeatable security control. When the team finds a vulnerability during an assessment, it can create a rule, explore variants, and look for similar issues in other relevant projects. This process extends security knowledge beyond the original review. A vulnerability found manually in one application can inform automated detection elsewhere, supporting the team's goal of scaling AppSec through reusable controls.

The workflow also connects manual and automated AppSec work. A focused assessment can uncover a pattern that generic scanning did not capture precisely enough. The team can encode that pattern, test it, and extend the check to projects where the same implementation risk may exist.

> "The dashboard is nice, but it wasn't the driver for us. The API was valuable because I can get the data, filter it the way we need, and send it where people already look at it."
>
> **Andrii Kudiurov**
> Senior AppSec Engineer, Docplanner

Integrating Semgrep into existing security reporting

Beyond reporting, Docplanner ingests Semgrep static analysis and AI-based findings into internally developed AI-assisted security assessment workflows. The team uses application-specific context to analyze potential impact across interconnected systems and user journeys. Semgrep pull-request comments also help developers and AI coding agents identify and respond to security findings in their existing workflows.

The Semgrep dashboard was not a deciding factor for Docplanner. The company already had a data team and a shared reporting environment. What mattered was the ability to retrieve Semgrep data through APIs, filter and deduplicate it, and send it to the systems where internal teams already consume security information. That lets AppSec incorporate Semgrep into the company's broader security data model without creating a separate reporting destination. This is particularly important because Docplanner measures performance across its broader AppSec program rather than attributing program-level results to individual scanners.

> "The things that we like in Semgrep, we like a lot. When it comes to speed of integration, ease of deployment, and ease of management, it just works."
>
> **Andrii Kudiurov**
> Senior AppSec Engineer, Docplanner

Bringing security closer to developers and coding agents

Docplanner is exploring how to move security checks closer to where developers and coding agents work. The team is evaluating deeper IDE integrations and reusable agent workflows that can run Semgrep reliably, support rule writing and variant analysis, and send new rules to the Semgrep platform.

For Docplanner, the next phase builds on the same operating model that guided its Semgrep deployment: automate wherever possible, give AppSec the control needed to maintain signal quality, and make security practical for hundreds of code contributors. Semgrep provides a centralized foundation the team can manage and extend as development workflows evolve.

About Semgrep

Semgrep enables organizations to identify and address security vulnerabilities in application code, open-source dependencies, and secrets. Its AI-assisted AppSec platform helps security teams reduce noise, prioritize meaningful risks, and integrate security into development workflows.

© Semgrep 2026