aws marketplace

Semgrep

Reviews, tips, and advice from real users

Powered by PeerSpot

Contents

Product Recap

Semgrep

Semgrep Recap

Semgrep is an advanced static analysis tool designed to identify vulnerabilities and enforce coding standards, catering primarily to professionals with a focus on enhancing code security and quality.

Engineered for software development environments, Semgrep delivers efficient security feedback with minimal setup. By offering a rich collection of rule sets, it allows customization and integration into CI/CD pipelines, supporting continuous code examination. Semgrep not only uncovers hidden flaws but also enforces best practices, making it a valuable asset for development teams seeking to build secure and reliable software.

What are the most important features of Semgrep?

- Customizable Rules: Allows users to define specific rules to match unique coding requirements.
- Open Rule Repository: Provides access to a vast array of pre-defined rules covering common security issues.
- CI/CD Integration: Seamlessly integrates into development workflows, providing immediate feedback.
- Multi-language Support: Detects issues across different programming languages, enhancing its usability.

What benefits or ROI should users consider?

- Enhanced Security Posture: Elevates the security standards of codebases.
- Time Efficiency: Reduces time spent on manual code reviews.
- Adaptability: Easily adapts to evolving coding standards and practices.
- Cost-effectiveness: Minimizes the need for external security audits.

In industry applications, Semgrep is a popular choice for sectors such as finance and healthcare, where code integrity and security are paramount. Its integration capabilities allow for effective oversight of compliance and secure coding standards without disrupting existing workflows. This adaptability ensures it meets sector-specific requirements, making it a trusted tool in fields where data privacy and protection are critical.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- "Compared to other competitors in the market, the AI-backed capability is the biggest strength of Semgrep."

Manjunath Maneppagol

Cloud & Application Security at Sixt SE

- "Semgrep flourishes with the SAST, secret scanning, and Software Composition Analysis types of scanning."

Verified user

DevSecOps Security Engineer at a manufacturing company with 10,001+ employees

- "The best part of Semgrep is its ease of integration with CI/CD pipelines and how it is a developer-friendly tool."

Francisco Javier Vergara

SecOps Engineer at IriusRisk

“The most valuable feature is the ability to write our custom rules.”

Henry Mwawai

Security Consultant | Application Security at Jowatechs

What users had to say about valuable features:

“Semgrep flourishes with the SAST, secret scanning, and Software Composition Analysis types of scanning. That is where Semgrep shines. With SCA, it helps find vulnerabilities, SAST weaknesses, and secrets. These are three existing services that are there in my enterprise, and we have other tools that perform the same. Semgrep, as I said, helps us benchmark that while running POCs.

“The Software Composition Analysis is the most valuable feature in Semgrep..”

Verified user

DevSecOps Security Engineer at a manufacturing company with 10,001+ employees

Read full review

"The best part of Semgrep is its ease of integration with CI/CD pipelines and how it is a developer-friendly tool. The interface is really focused on presenting developers what needs to be done, what vulnerabilities have been found, and what packages are affected. Whenever a developer enters the application, they do not need much context because it is really clear what needs to be done based on what the application shows.

Semgrep removes a lot of stress from the product security team since there is now an automated way of checking for vulnerabilities in our software. It has reduced manual work and saved a lot of time since containers no longer need to be manually checked with Semgrep, and we do not even need to check whenever there is a new version. In our automated pipelines, every time there is a new version, the containers get scanned and if something critical or high is detected, we are automatically notified.

Semgrep is scalable and works well across multiple repositories and projects, especially when integrated with CI/CD pipelines as is our case.."

Francisco Javier Vergara
SecOps Engineer at IriusRisk

Read full review

“The seamless integration of Semgrep into our existing platform is what I really appreciate. It is very easy, I was able to integrate and onboard it in just 10 to 15 minutes. This is in stark contrast to dealing with different SAST tools about integration across thousands of repos.

Another great feature is that Semgrep greatly reduces the noise compared to other SAST tools. After scanning through the codebase and understanding it, Semgrep has a capability called AI analysis or AI triage. When you triage with AI, it gathers context around the finding and reduces the noise about 80 to 90 percent of the time, asking you to focus only on findings that really matter.

Another excellent experience I had with Semgrep is when there was a finding that AI was not able to correctly diagnose or identify whether it was an actual finding or not. It reported it as a vulnerability, but when I verified it as a security engineer, I determined it was not a vulnerability in our case because we have compensatory controls in place. When I indicate this, Semgrep asks if it can apply the same logic to other similar findings. With a single click, it reduces a lot of noise for me, saving a huge amount of my time and effort.

The results are also impressive. Most solutions identify a static query like raw SQL and simply say there is a SQL injection that is critical. Semgrep, however, looks into the query file and understands the context. It recognizes that this is a SQL query without any user input or database migration script, and it assigns appropriate risk. This intelligent capability of Semgrep is what impressed me.

Semgrep will easily fit into the ecosystem you are building or the ecosystem you are working with. It is going to increase the developer experience in terms of how easily developers are able to understand the findings. It will also increase the security posture because developers are easily able to understand and fix those findings. Overall, the application security posture and the relationship between the development community and the security engineering will improve because Semgrep integrates so seamlessly and functions very smoothly. .”

Manjunath Maneppagol
Cloud & Application Security at Sixt SE

Read full review

ROI

Real user quotes about their ROI:

“Although there are no metrics available, an improvement in efficiency has been seen since manual labor is not required as much as before. This can be translated to being able to do the same amount of work with less technicians..”

Francisco Javier Vergara
SecOps Engineer at IriusRisk

Read full review

Use Case

“We use Semgrep to check custom user pipelines and test their claims for any vulnerabilities. We process the code by passing it through the testing process for any operability issues before sending feedback to the developers and providing the final product. This is part of the static testing analysis of code analysis..”

Henry Mwawai
Security Consultant | Application Security at Jowatechs

Read full review

“I use Semgrep mainly for its software composition analysis capabilities to identify vulnerabilities in dependencies used in our applications. Every time a new feature is developed or a new version of an application is released, it is run against Semgrep using our CI/CD pipelines to identify any new vulnerabilities..”

Francisco Javier Vergara
SecOps Engineer at IriusRisk

Read full review

"I have used Semgrep more as a testing and a POC tool. So, there is no consistent usage of Semgrep, but I have used the tool multiple times for POC purposes.

"As a DevSecOps Security Engineer, my main use case for Semgrep when I do use it for POCs or testing is to deal with SAST, secret scanning, and types of testing, white-box testing, AppSec, and those types of activities. Semgrep is a tool for that. Hence, when we perform POCs and try to understand what it is providing for such different types of scanning, Semgrep turns out to be useful in setting benchmarks.."

Verified user

DevSecOps Security Engineer at a manufacturing company with 10,001+ employees

Read full review

"I have been working with Semgrep for almost a year, approximately six to eight months on and off. In my current organization, I have a strong experience for SAST solution POCs, and I have conducted POCs for Semgrep, Checkmarx, Snyk, and SonarQube to evaluate SAST capabilities.

Our primary use case for Semgrep is to identify static code vulnerabilities and SAST vulnerabilities. Every other organization or vendor claims to offer this capability, but Semgrep is built differently compared to all these traditional tools. I have almost a decade of experience using various SAST tools, and Semgrep not only looks at particular code but understands the entire code to get context around whether an issue is real or not through context analysis.

One of the primary use case for us is also the shift-left approach, which means improving our developer experience. Our developers do not want to wait until they commit changes to GitHub or build it. They want synchronous feedback directly within their IDE. Semgrep provides an IDE integration and also supports MCP gateway. Additionally, secrets scanning is another important use case for us. ."

Manjunath Maneppagol
Cloud & Application Security at Sixt SE

Read full review

Setup

The setup process involves configuring and preparing the product or service for use, which may include tasks such as installation, account creation, initial configuration, and troubleshooting any issues that may arise. Below you can find real user quotes about the setup process.

"The setup was quite straightforward and the pricing model is quite flexible. The setup at the beginning was quick, and our pipelines were managed to be running easy enough and fast enough.."

Francisco Javier Vergara

SecOps Engineer at IriusRisk

Read full review

"The initial setup was straightforward, involving connecting the digital product to Semgrep. I am mainly involved in the usage aspect, and thus, I provided information from my perspective.."

Henry Mwawai

Security Consultant | Application Security at Jowatechs

Read full review

Customer Service and Support

“There was some difficulty in hearing the questions due to static noise, implying potential issues with communication or support on the call. However, rejoining the call resolved the problem..”

Henry Mwawai
Security Consultant | Application Security at Jowatechs

Read full review

Other Advice

“The first thing you need to do is to integrate Semgrep with your CI/CD pipelines and once they are running, invest time in reading documentation and getting yourself familiar with all of the products offered and all of the capabilities available. Semgrep was found through the peer link navigator that was provided via a LinkedIn message. The overall review rating for this product is 6 out of 10..”

Francisco Javier Vergara
SecOps Engineer at IriusRisk

Read full review

"You should primarily focus on what your use case is and why you are moving out. If you are moving out just from the perspective of cost, I do not think Semgrep is the best solution for you. However, if you are looking for value for investment and want to have the complete visibility into your code with less noise, if you are not just looking for a SAST but are really looking for actionable results and want to improve your developer experience and feedback, then you should go for Semgrep. In my organization, it is not only me who selects the solution; I bring in developers from junior and senior levels of all experience and ask them to take a hands-on experience and give me feedback. If you want to improve the developer experience, then go for Semgrep.

Compared to other competitors in the market, the AI-backed capability is the biggest strength of Semgrep. The seamless integration is another major advantage because I have done it for a few other solutions, some of which are extremely difficult and some are okay, but the Semgrep integration with the code repository was the smoothest. The quality of results and reduction in noise are also strengths compared to other competitors. Semgrep also has a great strength in the number of rule sets they have compared to all other vendors. While all other vendors have very limited numbers even though they claim to be enterprise, their community edition itself has close to 4,000 rules and the enterprise edition has around 20,000 rules. That is a really strong advantage.

As for limitations, I would say that Semgrep currently just supports Jira and Slack for integrations. They should expand to different integrations like ServiceNow and other CNAP and CSPM solutions where all results can be brought into one place.

I would rate this review an 8 out of 10. ."

Manjunath Maneppagol
Cloud & Application Security at Sixt SE

Read full review

Top Industries

by visitors reading reviews

Financial Services Firm 16%

Manufacturing Company 11%

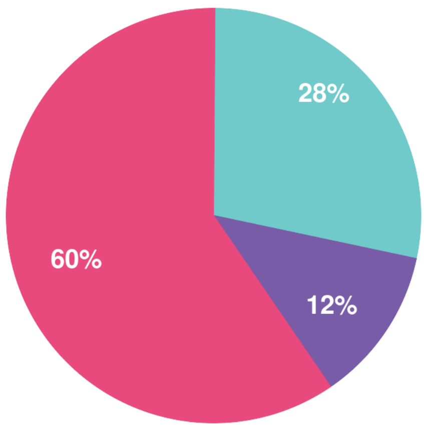
Computer Software Company 8%

Comms Service Provider 7%

Company Size

by reviewers

by visitors reading reviews



Large Enterprise Midsize Enterprise Small Business

About this buyer's guide

Thanks for downloading this PeerSpot report.

The summaries, overviews and recaps in this report are all based on real user feedback and reviews collected by PeerSpot's team. Every reviewer on PeerSpot has been authenticated with our triple authentication process. This is done to ensure that every review provided is an unbiased review from a real user.

Get a custom version of this report... Personalized for you!

Please note that this is a generic report based on reviews and opinions from the collective PeerSpot community. We offer a customized report of solutions recommended for you based on:

- Your industry
- Company size
- Which solutions you're already considering

The customized report will include recommendations for you based on what other people like you are using and researching.

Answer a few questions in our short wizard to get your customized report.
Get your personalized report here

About PeerSpot

PeerSpot is the leading review site for cloud, AI, and business software. We created PeerSpot to provide a trusted platform to share information about software, applications, and services. Since 2012, over 22 million people have used PeerSpot to choose the right software for their business.

PeerSpot helps tech professionals by providing:

- A list of products recommended by real users
- In-depth reviews, including pros and cons
- Specific information to help you choose the best vendor for your needs

Use PeerSpot to:

- Read and post reviews of products
- Access over 30,000 buyer's guides and comparison reports
- Request or share information about functionality, quality, and pricing

Join PeerSpot to connect with peers to help you:

- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendor

Visit PeerSpot: www.peerspot.com

PeerSpot

244 5th Avenue, Suite R-230 • New York, NY 10001

reports@peerspot.com

+1 646.328.1944