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 has positively impacted our organization by improving code quality and helping us eliminate vulnerabilities in our code."

Akashkhurana Hirana
Senior Software Engineer 2 at Porch

- "Since implementing Semgrep, I have noticed significant outcomes, for example, I can resolve vulnerabilities that previously took four days in under a day, saving both time and money, thus enhancing our return on investment."

Olakunle Obasoro
DevOps Engineer at Exponential Craft

"The feature is easy to use, saves a lot of time, and is streamlined in nature."

Verified user

Security Researcher at a tech vendor 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 Pulido

SecOps Engineer at a real estate/law firm with 501-1,000 employees

"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

"In my team, we use Semgrep, which is more efficient for coding purposes, time-saving, and quickly detects issues, and I can say that weekly I save about six to seven hours because of this, making it very time-saving and fostering faster development for my team's products and environment."

Hiten Nandasana

Angular developer at Flourish software

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 Pulido
SecOps Engineer at a real estate/law firm with 501-1,000 employees

Read full review

"First, it is very easy to use. It has customization features that allow me to customize it to find particular types of vulnerabilities that I am looking for. There is scanning efficiency which allows for rapid issue detection early in the development process. The customizable rule engine is the best thing because I can customize it according to my needs.

I can customize my rules according to my needs. The YAML file is easy to write. A person with good basic knowledge of coding can generate custom rules particular to the type of vulnerability they are targeting. Therefore, it is customizable.

The feature is easy to use, saves a lot of time, and is streamlined in nature. That is the best aspect.

It has helped my code review part significantly. It saves around two to three hours per day of going through each line of code to find mistakes and identify issues that are present at the code level. Code review is a tedious task for any security engineer or developer to do, so it helps tremendously while reviewing code.

By avoiding these tedious tasks, my team gets to focus on other important tasks that are required. Sometimes there are urgent tasks that need to be done before code reviews can be completed. The time I save is utilized elsewhere, which effectively benefits my team.."

Verified user

Security Researcher at a tech vendor with 10,001+ employees

Read full review

“Some of the best features Semgrep offers include its capability to integrate with over 30 languages. Our eight repositories consist of Java, Python, Node, and JavaScript. It operates very fast by creating an index to find changes rather than analyzing the entire repository on each commit, thereby scanning large codebases in minutes. Additionally, we can create our own pattern-based rules, which is an essential feature for us.

“Setting up custom pattern-based rules is easy, and we use them often for our team's needs. There is no specific coding language or technical skill required; we only need to create a YAML file, which anyone can write and use.

“Furthermore, Semgrep can integrate with Integrated Development Environments such as VS Code or IntelliJ. Some of the latest IDEs allow integration, enabling developers to scan the entire codebase directly from their development environment, so it is not only restricted to the CI/CD pipeline.

“Semgrep has positively impacted our organization by improving code quality and helping us eliminate vulnerabilities in our code. It allows for faster development since it autonomously reviews repositories and identifies vulnerabilities before a human review, leading to enhanced code quality and automated security testing..”

Akashkhurana Hirana
Senior Software Engineer 2 at Porch

Read full review

"The best feature of Semgrep is its ability to highlight high priority issues during scanning, making it critical for developers to address these vulnerabilities promptly. This seamless process enhances efficiency and expedites issue resolution within our systems.

"I find Semgrep's user-friendliness valuable, allowing me to run scans easily with simple commands, which clearly indicate vulnerabilities and their priority levels, effectively meeting my needs.

"When receiving high-priority findings, I act as a DevOps person who incorporates security into my culture by notifying developers about issues I find and urging them to check the code. I advocate that all developers have Semgrep installed on their laptops, ensuring they avoid pushing vulnerable code.

"The impact of Semgrep on my organization includes the recommendation I made as an external consultant to incorporate it into projects. It is easy for developers to use and helps monitor our security posture by scanning code before production pushes.

"Since implementing Semgrep, I have noticed significant outcomes. For example, I can resolve vulnerabilities that previously took four days in under a day, saving both time and money, thus enhancing our return on investment.."

Olakunle Obasoro
DevOps Engineer at Exponential Craft

Read full review

“In my current situation, when I work on any features or products, I find issues during my development phase while writing code. I can detect issues in a very early phase, which allows us to prevent forwarding them to production.

“This is very helpful for our development phase and it is very fast for our development process. I can save more time for developing and reviewing code, which makes it very helpful for our organization.

“Regarding Semgrep, I find it to be very user-friendly, easy to understand, and easy to integrate with any working tool. We use VS Code, and it integrates seamlessly with it. Additionally, I set up the CI/CD pipeline for the development phase, and it works well for all our needs.

“In my opinion, the best features Semgrep offers are for security vulnerability detection. I can find any vulnerabilities during my development phase, which helps my work and has many time-saving features.

“Whenever I use Semgrep, I have integrated it seamlessly into my experience. It integrates when I work with the development phase and the deployment model, allowing me to detect any security issues. I can detect these issues early and fix them as soon as possible, eliminating the need for manual line-by-line code checks. It quickly scans all the code and detects issues, saving me significant time.

“It can help my team very quickly, especially with large-scale projects. In my team, we use Semgrep, which is more efficient for coding purposes, time-saving, and quickly detects issues. I can say that weekly I save about six to seven hours because of this, making it very time-saving and fostering faster development for my team's products and environment..”

Hiten Nandasana
Angular developer at Flourish software

Read full review

Other Solutions Considered

"Previously, we used SonarQube, but we switched because SonarQube is oriented more towards bug fixing and lacks the focus on security analysis we needed.."

Akashkhurana Hirana
Senior Software Engineer 2 at Porch

Read full review

"Previously, I used the SonarQube solution but switched to Semgrep because Semgrep works faster and the code scannability is very good compared to SonarQube.."

Hiten Nandasana
Angular developer at Flourish software

Read full review

"If you are looking for an open-source tool that can perform SAST in your environment and you are a technical person with a team that can grasp new technologies in a short period of time, then you can use Semgrep directly to perform SAST and code reviews at the development level. Early detection of security issues and bugs can be fixed.."

Verified user
Security Researcher at a tech vendor with 10,001+ employees

Read full review

"I have used SonarQube. However, the results of Semgrep are much better. I compared them both, so I switched to Semgrep only, and it works very well. I do not have to pay any licensing fee or anything like that. It has been good to work with Semgrep.

I evaluated a tool such as SonarQube, which is in the market and is also open-source. However, the results provided by Semgrep are much more effective and efficient with fewer false positives. The number of true positives is higher, which effectively saves time from checking whether false positives are right or wrong.."

Verified user

Security Researcher at a tech vendor with 10,001+ employees

Read full review

ROI

Real user quotes about their ROI:

"The return on investment is very evident. I can say it saves us time related to coding and also saves money, making it a very reliable tool for our organization with great features.."

Hiten Nandasana
Angular developer at Flourish software

Read full review

"The return on investment from using Semgrep is evident as I save time and money. For example, tasks that previously took days are completed in significantly less time, enabling faster business responses and improved profit margins.."

Olakunle Obasoro
DevOps Engineer at Exponential Craft

Read full review

"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 Pulido
SecOps Engineer at a real estate/law firm with 501-1,000 employees

Read full review

Use Case

"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 Pulido
SecOps Engineer at a real estate/law firm with 501-1,000 employees

Read full review

"My main use case for Semgrep is as a SAST tool. Since I work with code directly, I use it to scan the code for vulnerabilities and relay information to developers so they can address any issues. This approach ensures I maintain a security focus as a DevOps person, which is crucial.

"Semgrep fits into my workflow by allowing me to scan code and ensure there are no breaches before running it in containers.."

Olakunle Obasoro
DevOps Engineer at Exponential Craft

Read full review

"My main use case is to perform SAST, static application security testing. I have been using it for the last 10 months. Initially, I was planning to use it just for the code review part so that developers can get secure code. However, it can also be integrated in CI/CD pipelines and other tools, which makes it robust.

I deployed Semgrep with my development team in their IDEs, such as VS Code and other notebook tools that my developers use. Semgrep helps to identify code-level issues, such as the possibility of SQL injection, XSS, or hard-coded values. It initially triggers alerts and shows which aspects are not correct and need correction.."

Verified user
Security Researcher at a tech vendor with 10,001+ employees

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

"My primary use case for Semgrep is for day-to-day code scanning and code reviewing during development, focusing on vulnerability detection. I am also migrating this tool into our CI/CD pipeline.

"The primary objective is to scan code, detect vulnerabilities, and integrate into CI/CD pipelines during the coding phase before deployment to production so we can identify all issues in the development phase.

"I currently use Semgrep for our development process, CI/CD pipeline, and vulnerability detection, and it is a very good product.."

Hiten Nandasana

Angular developer at Flourish software

Read full review

"Semgrep serves as an open-source static application security testing tool for my organization. We work under a microservices model with multiple repositories, around eight in total. Whenever we make any code changes, Semgrep scans the whole repository, trying to find security vulnerabilities, bugs, or coding standard violations that might have been missed before peer-to-peer review. It gives us security scanning results and allows us to implement custom rules created in Semgrep, which is integrated with our CI/CD pipeline, such as Jenkins or GitLab. Whenever a pull request is made, Semgrep scans the entire repository and identifies security bugs and code vulnerabilities before any human review.

"A quick specific example of how Semgrep helped me catch something important is when we were using Java across multiple repositories while utilizing GCP tokens as our cloud provider. In one of our pipeline files, someone printed a private key token in the console during a pull request review. Semgrep flagged this issue, alerting us that this private key was vulnerable and should never be printed in the console. This was caught before it reached production. Additionally, Semgrep suggested best practices such as encrypting passwords before saving them, which were enhancements we previously overlooked.."

Akashkhurana Hirana
Senior Software Engineer 2 at Porch

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 Pulido

Read full review

SecOps Engineer at a real estate/law firm with 501-1,000 employees

"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

Read full review

Information Security Engineer at a consultancy with 11-50 employees

Customer Service and Support

"Concerning customer support, I have not had any use cases that required assistance. However, the documentation is excellent. When I created custom rules, I had some doubts, and the documentation was very helpful, simple, and easy to understand.."

Akashkhurana Hirana
Senior Software Engineer 2 at Porch

Read full review

"Customer support and services for Semgrep are very reliable and good. Many times when I have had troubleshooting needs, I find most solutions in the documentation, so the support and customer service team is excellent.."

Hiten Nandasana
Angular developer at Flourish software

Read full review

"Customer support is good because I have not needed much customer support until now, which is very good. I think that is a good part. Their documentation and community are very active, so most of the time when problems occur, I get a solution.."

Verified user
Security Researcher at a tech vendor with 10,001+ employees

Read full review

"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
Information Security Engineer at a consultancy with 11-50 employees

Read full review

Other Advice

"It streamlines with the governance and compliance of the country where the company operates. It follows GDPR guidelines and EU guidelines. In India, I follow certain guidelines, so it also passes that criteria to go through those guidelines and follow the restrictions and suggestions provided at a national level. ."

Verified user
Security Researcher at a tech vendor with 10,001+ employees

Read full review

"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 Pulido
SecOps Engineer at a real estate/law firm with 501-1,000 employees

Read full review

"I would not want to see anything changed.

"My advice for others considering Semgrep is that it is a very good product and a great tool to use. It has a very user-friendly environment and it is very time-saving, as I mentioned earlier. I do not have any additional thoughts about Semgrep. My overall review rating for Semgrep is nine out of ten.."

Hiten Nandasana
Angular developer at Flourish software

Read full review

"My advice for others considering Semgrep is to adopt it, as it stands out in the open-source market and shows solid growth. You can trust it based on its innovative developments.

"I believe Semgrep will scale effectively with the rise of agentic AI and security needs, leading to broader adoption among companies. Sharing wins at open-source conferences will help demonstrate its potential impact.

"I rate this review an 8.."

Olakunle Obasoro
DevOps Engineer at Exponential Craft

Read full review

"Although not directly in the development process, Semgrep has saved substantial time in the review process. For instance, when a developer raises a pull request, Semgrep automatically reviews it before another developer or manager does. This saves a lot of time in reviewing features. Semgrep has detected over 150 vulnerabilities across our eight repositories, and it takes minimal time to scan the

full repository, which is one of its best aspects.

“I would rate Semgrep a 9 out of 10. I chose a nine out of ten mainly because of the occasional false positive results I mentioned earlier; that is the only thing preventing me from giving it a full score.

“Regarding Semgrep's AI capabilities, it serves as a security tool to check for vulnerabilities in code. From my experience, it has successfully identified over 150 security vulnerabilities in our code, and I find it completely reliable in terms of security.

“My advice for others considering Semgrep is that if you have large repositories, there are very few tools on the market that can provide security scanning and identify vulnerabilities quickly. Semgrep is one of those tools that performs very efficiently. If security is a concern for you, I recommend trying the free version first; if it proves beneficial for your organization, then make an organizational decision to onboard it..”

Akashkhurana Hirana
Senior Software Engineer 2 at Porch

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

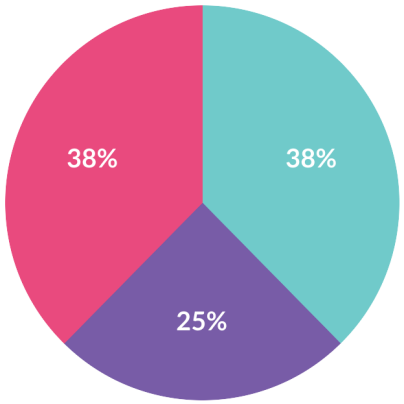
Top Industries

by visitors reading reviews

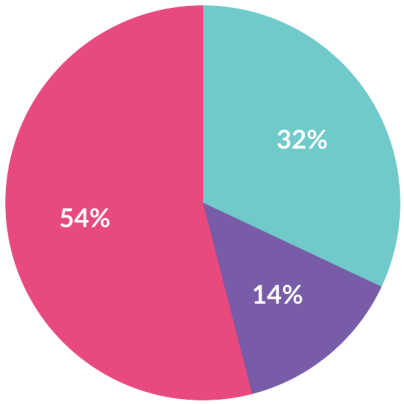
Financial Services Firm	14%
Manufacturing Company	10%
Comms Service Provider	9%
Outsourcing Company	8%

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