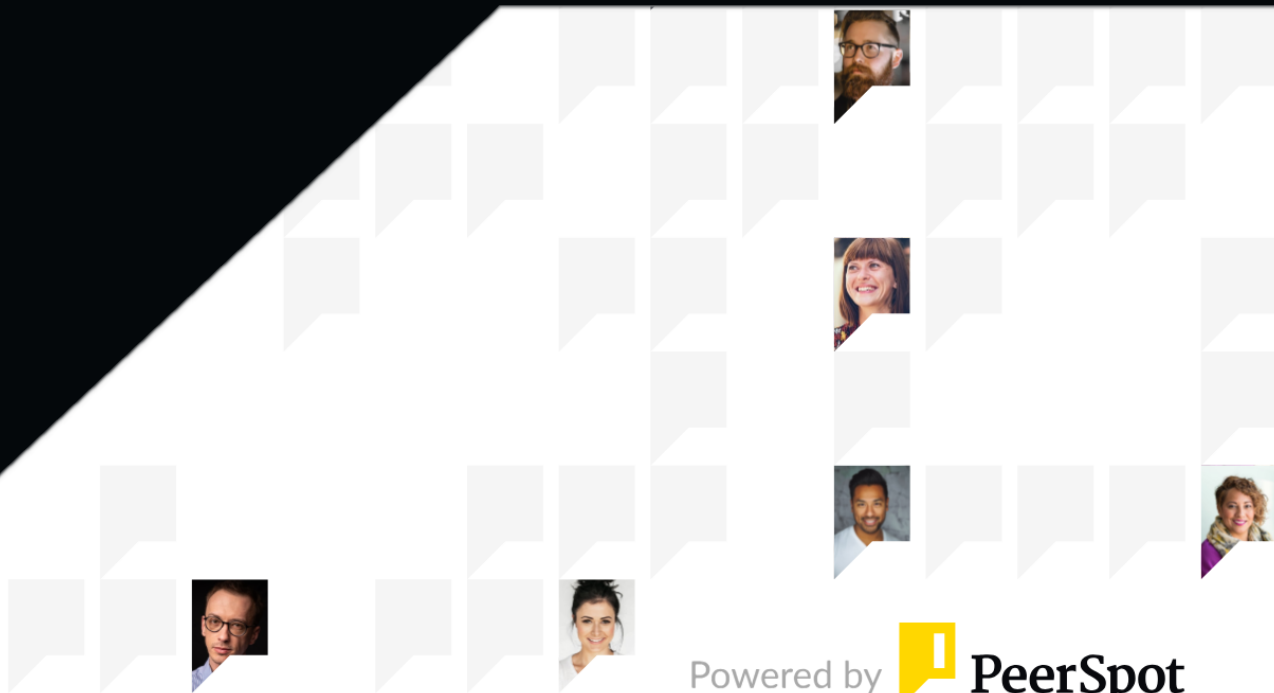


aws marketplace

Snyk

Reviews, tips, and advice from real users



Powered by  PeerSpot

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 10

Other Solutions Considered..... 11 - 13

ROI..... 14 - 18

Use Case..... 19 - 23

Setup..... 24 - 27

Customer Service and Support..... 28 - 30

Other Advice..... 31 - 35

Trends..... 36 - 37

About PeerSpot..... 38 - 39

Product Recap

snyk

Snyk

Snyk Recap

Snyk is a developer-centric security platform offering simplicity, self-service, and integration with source control and CI systems for effective vulnerability management.

Focused on enhancing developer productivity, Snyk provides a robust vulnerability database with accurate information, software composition analysis, and integration capabilities with IDEs, pipelines, and Slack for notifications. Its container security feature and automation offer prioritized vulnerability management. Users note areas for improvement such as adding SAST and DAST capabilities, expanding language support, refining reporting and notifications, and enhancing API and external system integration. UI speed and reducing false positives are additional concerns.

What Are Snyk's Key Features?

- **Extensive Integration:** Seamlessly integrates with source control, CI systems, and IDEs for streamlined workflows.
- **Accurate Vulnerability Database:** Provides reliable, up-to-date vulnerability information for better decision-making.
- **Container Security:** Facilitates secure and efficient management of container environments.
- **Actionable Advice:** Offers detailed guidance for prioritizing and addressing vulnerabilities.

What Benefits Can Users Expect?

- **Cost-Effectiveness:** Provides a high security level, enhancing risk management without excessive expenditure.
- **Ease of Use:** Designed to be intuitive for developers, facilitating quick adoption and efficient workflows.
- **Continuous Monitoring:** Enables ongoing surveillance of dependencies and environments for emerging threats.

Snyk is leveraged in industries for secure code review and compliance assurance, integrating into development pipelines to monitor open-source libraries, Docker images, and Kubernetes deployments. Its integration with tools like GitHub and Jenkins aids teams in timely vulnerability identification and management, enhancing security practices.

Valuable Features

Excerpts from real customer reviews on PeerSpot:



“Snyk has positively impacted my organization by improving the security posture across all software repositories, resulting in fewer critical vulnerabilities, more confidence in overall product security, and faster security compliance for project clients.”



Abhishek-Goyal

Software Engineer at a computer software company with 11-50 employees



“Across the initiative, that translated into thousands of developer hours saved and the equivalent of one to three full-time developers of effort reallocated to feature work instead of bug or patchwork.”



Boya Uday Kumar

Ai Research Enthusiast And Developer at ADP



“Snyk is paramount and extremely important for us because anything that goes to production should not have any security vulnerabilities, and every application that goes into production must pass Snyk vulnerability scanning before it can be deployed.”



KannanPadmanabhan

Senior Software Engineering Manager at a financial services firm with 10,001+ employees



“The best feature of Snyk is the integration with our ticketing system, which is Jira.”



Verified user

Information Security Strategy at a insurance company with 10,001+ employees



“The most important feature of Snyk is its cost-effectiveness compared to other solutions such as Check Point.”



meetharoon

CEO at a computer software company with 10,001+ employees



“They evolved their maturity because they could find the vulnerabilities before the pipeline runs.”



ANDRESANTOS

Senior DevSecOps at V8



“Snyk provides a lot of information on vulnerabilities, the packages being used, and their dependencies, giving good insight into the security of those packages.”



PawanSingh2

Director at Marsh

What users had to say about valuable features:

“Snyk is finding all the issues we have. It suggests solutions for every vulnerability, and we are getting patches frequently. As someone from an enterprise, I want to share feedback that might help others. There are multiple teams involved in our organization. We have a separate cyber team that works with Snyk and keeps on updating, though I am not fully aware of all the details in that area..”

KannanPadmanabhan

[Read full review](#) 

Senior Software Engineering Manager at a financial services firm with 10,001+ employees

“The best feature of Snyk is the integration with our ticketing system, which is Jira. That integration was one we were specifically looking for. The deep integration with our IDE and repository is another valuable feature. In terms of deploying these features, it's seamless..”

Verified user

[Read full review](#) 

Information Security Strategy at a insurance company with 10,001+ employees

“The most important feature of Snyk is its cost-effectiveness compared to other solutions such as Checkmarx. It is easy to consolidate Snyk across multiple entities within a large organization.

Additionally, our integration of Snyk into GitHub allows us to automatically scan codebases and identify issues, which has improved efficiency..”

meetharoon

CEO at a computer software company with 10,001+ employees

[Read full review](#) 

“I appreciate the UI. It is simple, fast, and I value the precision in the tests. The responses are positive.

“Regarding the vulnerability database and AI, we have good experience with that. I cannot compare with other providers or vendors such as Veracode, Checkmarx, and others. All the tests are positive in my analysis..”

ANDRESANTOS

Senior DevSecOps at V8

[Read full review](#) 

“Snyk's main features include open-source vulnerability scanning, code security, container security, infrastructure as code security, risk-based prioritization, development-first integration, continuous monitoring and alerting, automation, and remediation. The best features I appreciate are the vulnerability checking, vulnerability scanning, and code security capabilities, as Snyk scans all open-source dependencies for known vulnerabilities and helps with license compliance for open-source components.

Snyk integrates into IDEs, allowing issues to be caught as they appear in the code dynamically and prioritizes risk while providing remediation advice.

Snyk provides actionable remediation advice on where vulnerabilities can exist and where code security is compromised, automatically scanning everything and providing timely alerts.

Snyk has positively impacted my organization by improving the security posture across all software repositories, resulting in fewer critical vulnerabilities, more confidence in overall product security, and faster security compliance for project clients.

Snyk has helped reduce vulnerabilities significantly. Initially, the repository had 17 to 31 critical and high vulnerabilities, but Snyk has helped manage them down to just five vulnerabilities, which are now lower and not high or critical..”

Abhishek-Goyal

[Read full review](#) 

Software Engineer at a computer software company with 11-50 employees

“I find the most useful features of Snyk to be vulnerability scanning for code dependencies, containers, and infrastructure as code, with dependency intelligence that helps identify risky open-source packages and transitive issues. In major corporations like ADP, dependency intelligence is something that we actually care a lot about. I also like the fixed guidance feature, which includes upgrade suggestions and automated fixed pull requests. It has a developer-friendly workflow, so security issues show up where engineers already work, which is Visual Studio. We, as a team, appreciate two other important features: continuous monitoring, which helps us track risks even after the initial scan, and prioritization, allowing us to focus on the most important issues first.

“Dependency ingestion helps us see not just the direct package with the issue but also the transitive dependencies underneath it, which matters a lot because many security problems hide in nested libraries. Without that visibility, we might just miss the real root cause. It also helps the team judge whether a vulnerability is actually relevant to our application or just something we can safely deprioritize, saving us a lot of time during upgrades and migration work. Regarding fixed guidance, it is so valuable because it turns the scan result into an action. Instead of just telling us something is vulnerable, it often points us towards a safer version, an upgrade path, or a remediation option that we can apply quickly. That makes the team faster because developers do not have to investigate every issue from scratch, reducing back and forth between development and security review.

“Snyk had a very positive outcome on ADP and our workforce. The biggest positive outcome is less time spent on security remediation and fewer vulnerabilities carrying forward into later stages. Snyk's own metrics framework tracks open issues, new issues, resolved issues, PR checks, and time to fix, which maps well to the kind of benefits we saw in the Mythos initiative. The results included a 44% reduction in mean time to fix and a 62% reduction in critical vulnerabilities, along with an average of 2.2 development full-time employment worth of productivity gains. We saw a very positive impact mainly through time savings and earlier remediation as Snyk helped us catch vulnerabilities sooner during upgrades and migrations, reducing the effort for manual security issues. In practical terms, it improved a lot of developer productivity and helped the team fix security problems faster than ever with very little disruption..”

Other Solutions Considered

“Previously, we used Synopsys Coverity and later migrated to Checkmarx and Mend before Snyk. Synopsys Coverity was costly, prompting a switch. Snyk's affordability and consolidating capabilities across the entities led to its adoption..”

meetharoon

CEO at a computer software company with 10,001+ employees

[Read full review](#) 

“I did evaluate other options before choosing Snyk. I only considered Sonar before Snyk, but I ended up with Snyk because it's faster and more focused on security..”

NguyễnHuy

Student at VNU

[Read full review](#) 

“I made a proof of concept for a client with Checkmarx for about one month. I provided them a review about my experience. Now they are analyzing my results and considerations about other products too. I do not know if they already have a response about which product they will buy..”

ANDRESANTOS

Senior DevSecOps at V8

[Read full review](#) 

“It is simpler than other vendors. We have some difficulties with other license models. They are more complex and involve an acquisition of more products such as Synopsys and Checkmarx used a complex license model. Snyk has a license model simpler than most of the other vendors..”

ANDRESANTOS

Senior DevSecOps at V8

[Read full review](#) 

“Before choosing Snyk, we looked at a few alternatives, such as SonarQube and GitHub Advanced Security, which we were actually using previously. We switched to Snyk because we thought it would be easily integrated into our developer workflow. Snyk has very useful features and was particularly beneficial during the Mythos upgrade, leading us to switch to Snyk across the teams..”

Boya Uday Kumar

Ai Research Enthusiast And Developer at ADP

[Read full review](#) 

“Before Snyk, we used a mix of manual dependency checks, local static scans, and an older open-source scanner as our primary tooling, but we switched to Snyk because it had the coverage and accuracy. Snyk's vulnerability database and dependency intelligence catch more transitive and emerging issues than the older scanner we used. It also integrates easily into the developer workflow because we have an extension in VS Code that we could leverage, and it offers automated fixed PRs along with clear upgrade guidance, dramatically reducing the time spent on researching remediation steps compared with our previous approach. The enterprise readiness, continuous monitoring, and analytics were other aspects that helped us choose Snyk over other older tools..”

Boya Uday Kumar

Ai Research Enthusiast And Developer at ADP

[Read full review](#) 

ROI

Real user quotes about their ROI:

“I can see that Snyk saves the costs of hiring security developers for vulnerability scanning and security checks, as that responsibility is now managed by Snyk..”

Abhishek-Goyal

Software Engineer at a computer software company with 11-50 employees

[Read full review](#) 

“Snyk allows developers and development managers to identify open-source vulnerabilities in every stage. As a result, the fix is much cheaper than identifying something on production. It's up to 100 times less expensive. If you fix a few bugs at an early stage, you cover all the license fees for the annual subscription of Snyk. There is a high return on investment potential..”

ZvikaRonen

Chief Technology Officer at FOSSAware

[Read full review](#) 

“The more security that we have, the more confident we are. You never know when you will be actually attacked. Hopefully, this will not be validated anytime soon in reality. However, by doing our penetration tests, we are validating the system on a regular basis, which will also help improve our overall confidence in this area.

It gives us peace of mind that there is nothing hidden that hasn't been taken care of. That is also important.

The solution has reduced the amount of time it takes to fix and find problems..”

Verified user

[Read full review](#) 

Director of Architecture at a tech vendor with 201-500 employees

“I have seen a 70% ROI from Snyk. The other 15% is my company's fault. If you don't have your development team engaged to reduce all kinds of issues to zero, you are wasting some of your money. In the past, some squads didn't use the platform at all even though they had access, which is a waste of money because we could use the free solution instead. Some other squads engaged with calls trying to bring the number of issues down to zero. They worked so hard on the platform and got so deep into the documentation that they brought huge results.

For example, some of our projects had 25 critical and 100 high-level issues. My development team brought it down to 0 criticals and reduced 75% of the high-level issues by only using the tools on Snyk without asking me any questions, only looking at the platform and reading the solution on their own to find out what could be done to fix the problem.

I saw an ROI for some of my squads. For others, I only saw 20%. Seeing an ROI depends on the scenario in your company..”

Eryk Lawyd

Tech Lead DevSecOps at Letsbank

[Read full review](#) 

“If I didn't see ROI, I would move somewhere else. I would probably go to a cheaper solution, but Snyk is definitely above that compliance level of value. It is really proactive, and that's where I would rather be from a security program perspective. So, I do get the value out of it.

Snyk finds problems that we may not have ever found otherwise, so it is a significant benefit for us. It reduced the amount of time by an FTE, which is about 2000 hours a year that we would spend in doing what Snyk does with its tool.

Over the course of a year, Snyk has reduced the amount of time it takes to fix problems by approximately 100 hours in our enterprise. It makes it very clear what the fix is. They provide very good remediation advice.

The total time to value will depend on the company who implements it. For us, it was pretty short, probably two to three months. While it was very easy to set up, it takes a little while to really appreciate how its findings need to be addressed within the company. It forces you to develop some processes and feedback loops that you may not have had there before. So, it took us 90 days to fully appreciate the value and start remediating findings that were initially discovered..”

Sean McElroy

CISO at a tech vendor with 51-200 employees

[Read full review](#) 

“We definitely saw a measurable return on investment after adopting Snyk for the Mythos initiative, with the biggest wins being time savings and faster remediation. On average, we reduced the mean time to fix security issues by roughly 40 to 50% for the classes of vulnerabilities Snyk surfaced, which shortened our exposure window and reduced rework during upgrades. For ad hoc dependency issues and transitive vulnerability remediation, we estimate developer effort per vulnerability dropped from 8 to 16 hours down to about 2 to 4 hours, thanks to Snyk's dependency intelligence and automated fixed PRs. Across the initiative, that translated into thousands of developer hours saved and the equivalent of one to three full-time developers of effort reallocated to feature work instead of bug or patchwork.

“We also saw process benefits, with the number of critical, high-severity issues discovered late in testing or post-deployment dropping significantly. Roughly a 50 to 60% reduction for the targets we track, which reduced hotfix churn and decreased incident-related costs. Using Snyk in VS Code as an extension for CI pipelines meant many fixes were made pre-merge, and our PR blocking rate for high-risk vulnerabilities dropped, while the PR fix throughput increased. In terms of cost avoidance, faster fixes and fewer incidents reduced risk exposure and the potential remediation cost of production incidents. When combined with the time savings mentioned above, the team-level ROI is clear. The subscription cost is small compared to the developer hours recovered and reduced business risk during a major upgrade and migration program, so we saw a clear ROI, and it was very beneficial..”

Boya Uday Kumar

Ai Research Enthusiast And Developer at ADP

[Read full review](#) 

Use Case

“The main tool today is used to check for security issues in our products. We use it to analyze all the projects, and our security efforts are based partly on this tool..”

Diego Moreo

Software Quality Coordinator at a retailer with 10,001+ employees

[Read full review](#) 

“I lead a code security practice for our organization. We integrated Snyk into our GitHub, using CLI to automatically scan codebases and identify issues. We are a large organization with three independent entities, consolidating Snyk across all entities.

We also provide access through numerous CI/CD tools. Our default implementation mechanism is CLI, but we also use the Web UI for a comprehensive view and recommendations..”

meetharoon

CEO at a computer software company with 10,001+ employees

[Read full review](#) 

“I typically use Snyk for checking the security and vulnerabilities in my repositories.

Recently, I have used Snyk in one of my repositories for security and vulnerability checks, providing comprehensive knowledge about the repository, including what it does and where the security vulnerabilities are located.

I am using Snyk for the first time and did not use any vulnerability scanning solution before this. I was previously doing Red Hat vulnerability scanning locally for dependency checks, which was not what I wanted..”

Abhishek-Goyal

Software Engineer at a computer software company with 11-50 employees

[Read full review](#) 

“We are a customer of Snyk, which is a SaaS solution. We are one of the tenants using Snyk services but are not doing any enhancement development. We are purely a customer availing Snyk services.

“We are also using a separate DAST tool, though I am not aware of the tool name as it is managed by a different team.

“We utilize two main capabilities: application vulnerability detection and SCA capabilities. The primary reason we use Snyk is for SAST, as we want to scan our applications for any security vulnerabilities and address them..”

KannanPadmanabhan

Senior Software Engineering Manager at a financial services firm with 10,001+ employees

[Read full review](#) 

“The most recent client had experience with other products that did not have some features Snyk provides, such as Fortify in the old version before OpenText acquisition. They gave feedback about the precision in discovering vulnerabilities. They found that Snyk can provide more insights about vulnerabilities than older applications in SAST and SCA.

“We have integration with GitHub Actions to analyze the code and we use a double check in the pipeline. Our strategy is about shift left. The developers connect with Snyk, Git, and use this with the pipeline..”

ANDRESANTOS

Senior DevSecOps at V8

[Read full review](#) 

“My main use case for Snyk involves finding and fixing security issues during application upgrades and migrations. In my work at ADP, I primarily use it to scan applications for vulnerabilities, identify risky dependencies, and help the team remediate issues before they become production problems. We had an initiative called Mythos where we had to upgrade the application and fix all security issues, and Snyk was very helpful during that time.

“In one of the Mythos upgrades, Snyk highlighted a dependency vulnerability that was buried in the package chain, which was not something we would have caught quickly by manual review. Because it surfaced early, we fixed it during the upgrade itself instead of dealing with it later, which immensely reduced the risk and kept the rollout on track. That was one of the incidents that I had with Snyk, and it was absolutely very helpful during this complete Mythos upgrade for all the team members.

“Another important part of how Snyk fits into my workflow is that it helps shift security left. Instead of waiting until the end of a project to discover vulnerabilities, we can catch them while we are still upgrading, migrating, or making any code changes. It also fits well into the developer workflow because it is just another plugin that we have in Visual Studio Code to be enabled to ensure all security issues are scanned and displayed visually. Once that is done, we can fix it in a matter of time, so having it as an extension in Visual Studio Code is one of the important things for developers because it becomes easily integrated into the workflow they are working with..”

Boya Uday Kumar

Ai Research Enthusiast And Developer at ADP

[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 initial setup of Snyk is simple and straightforward compared to Synopsys Coverity, which is complex. Checkmarx falls in between, not too complicated or easy, but a reliable option. Snyk's ease of implementation makes it user-friendly..”

meetharoon

CEO at a computer software company with 10,001+ employees

[Read full review](#) 

“Snyk's initial setup is not very difficult.

On a scale from one to ten, where one is difficult and ten is easy, I rate the solution's initial setup a seven out of ten..”

Jayashree Acharyya

Director at PepsiCo

[Read full review](#) 

“The product's initial setup phase was easy.

The solution's deployment model varies from customer to customer. My company deals with a mix of clients, some of whom deploy the tool on the cloud while others deploy it on an on-premises model. .”

ManishSaxena

[Read full review](#) 

Devops & Cloud Architect at Hexaware Technologies Limited

“My experience with pricing, setup cost, and licensing is good, as the overall setup experience is smooth with easy onboarding for connection with GitHub and GitLab. I primarily use it with GitHub, requiring just a few clicks to set up Snyk..”

Abhishek-Goyal

[Read full review](#) 

Software Engineer at a computer software company with 11-50 employees

“I would rate the initial setup of Snyk a nine out of ten because it's straightforward. The web version is also easy to use. I'm working with both the web version and the IDE at the same time.

For deployment, I just link it to GitHub, upload the repository there and it automatically scans for any errors. It took around a minute to deploy Snyk.

.”

NguyễnHuy

Student at VNU

[Read full review](#) 

“I brought Snyk into the bank I work with. I held the technical interview, made a POC, and the initial commits and imports on the tool.

The initial setup's difficulty depends on whether you use it on CI/CD, but I rate it eight out of ten. The initial setup is not very hard, especially if you use the Snyk IO on the cloud platform. It is just point-and-click. If you are using it on your customizations, on your CI/CD, the rating drops to six out of ten because you need to understand very well what you need on your CI/CD staging to apply Snyk as the correct tool for that demand.

It took at least about 30 seconds to deploy Snyk on the platform. The authorization to break the pipeline takes at least 15 seconds.

The steps taken for deploying Snyk differ for each kind of solution and application we have here, but they follow the same recipe. First, we perform a SaTScan, to look for a hardcoded password or access key, then perform a unit test to see if the solution passes and then install. We check to see, "Oh, you have these kinds of issues." We might have high, critical, lower, or information issues. After that, we deploy the solution on the deployment environment, then repeat the same steps in staging the environment. After this, we make the build for the production site or environment..”

Eryk Lawyd

Tech Lead DevSecOps at Letsbank

[Read full review](#) 

Customer Service and Support

“The solution’s technical support team was involved during the architecture integration. We got their support, but I think we could probably get a faster response from them..”

Jayashree Acharyya

Director at PepsiCo

[Read full review](#) 

“We do not raise issues directly with Snyk. We have a common team that liaises with Snyk. Whenever we have issues, we raise them with the cybersecurity team within our company who supports Snyk, and they in turn interact with Snyk..”

KannanPadmanabhan

Senior Software Engineering Manager at a financial services firm with 10,001+ employees

[Read full review](#) 

“The documentation is good. It is one of the reasons we did not need support. We could understand the implementation of the product and other features without the need for human interaction..”

ANDRESANTOS

Senior DevSecOps at V8

[Read full review](#) 

“Our organization maintains a good relationship with Snyk's customer support team. Despite potential variations in service quality for smaller organizations, our long-standing association has ensured smooth communication, resulting in favorable support experiences and satisfactory issue resolution..”

meetharoon

[Read full review](#) 

CEO at a computer software company with 10,001+ employees

“We have contacted Snyk's technical support regarding several issues, and they have resolved them successfully.

“Snyk's technical support deserves a rating of seven or eight out of ten. Their response time aligns with their SLA commitments..”

Verified user

[Read full review](#) 

Information Security Strategy at a insurance company with 10,001+ employees

“Customer support has been decent overall. When we needed help as a team, we approached them, and they are generally responsive and knowledgeable, though the experience can vary depending on the support level. The documentation is very strong, which reduces the need to go to support teams in most cases. I would rate the customer support as a 9 out of 10 because they are mostly knowledgeable, and Snyk definitely has very good documentation, leading to very little chance of needing to contact customer support..”

Boya Uday Kumar

Ai Research Enthusiast And Developer at ADP

[Read full review](#) 

Other Advice

“Snyk is optimal for organizations starting or looking for an affordable, effective tool. Despite false positives, it combines [SAST](#), [SCA](#), containers, and IaS in one Web UI. On a scale of one to ten, I rate Snyk at six..”

meetharoon

CEO at a computer software company with 10,001+ employees

[Read full review](#) 

“My advice for others considering using Snyk is to rely on it for security issues but still manually review your overall code. It's great for detecting syntax errors but might miss some broader issues, so it's important to do a thorough check yourself.

Based on my experience, I'd rate Snyk an eight overall. Its performance is indeed good..”

NguyễnHuy

Student at VNU

[Read full review](#) 

“My advice for others looking into using Snyk is that if you are starting a repository that is free from vulnerabilities and security checks, Snyk is a good option. It automatically provides advice on how to improve for reducing vulnerabilities and security issues, allowing for easy removal of vulnerabilities. You can use it for a free trial, and if it impacts your organization positively, you can consider further usage.

Snyk is a very good product for vulnerability code scanning and can be used effectively. I would rate this product a nine point five out of ten..”

Abhishek-Goyal

Software Engineer at a computer software company with 11-50 employees

[Read full review](#) 

“My advice would be straightforward: start with a clear use case and test Snyk in the workflow where your developers actually work. It is strongest when it is used early in the SDLC, especially for application upgrades, dependency checks, and fixing security issues before they reach production. I also suggest using it in a real project first, not just a demo, and paying attention to the dependency intelligence and fixed guidance because that is where it saves the most time. Evaluating Snyk on a real project and focusing on how well it fits into your daily development workflow is key. It is especially useful for catching vulnerabilities early, so the more closely you integrate it into your process, the more value you get. I would rate Snyk an 8 out of 10 overall..”

Boya Uday Kumar

Ai Research Enthusiast And Developer at ADP

[Read full review](#) 

“While Snyk may not be the absolute best option in the market, it offers the most seamless experience currently available. Based on their price point and features, it's both affordable and fair considering the license package offered.

“During our implementation, we conducted a pilot test with Snyk for approximately two weeks during our UAT session. We spent an additional two to three weeks obtaining management approvals for production repository access. The testing was performed on development repositories before moving to production. While the actual implementation took about a week, the complete process duration was extended due to internal organizational approval processes.

“I rate Snyk 8 out of 10..”

Verified user

Information Security Strategy at a insurance company with 10,001+ employees

[Read full review](#) 

“I am from an enterprise and want to share feedback that might help others. There are multiple teams involved in our organization. I am from the application team, so I know the vulnerabilities and how to fix them. However, there is a platform team that takes care of giving permission for Snyk and access levels, which I am not fully aware of. At a high level, we have a Snyk admin team in our company that gives permissions, though I do not know all the details of what they do. I cannot share feedback on the admin area, but I can share that vulnerability-wise, I am happy with what Snyk provides and the solutions it gives.

“When Snyk identifies issues, our pull request process will not allow us to merge them in the first place. Snyk helps us by blocking critical issues and vulnerabilities. If someone bypassed the pull request check, we have another check in place before production release where we validate everything and block the code if it violates our standards. Based on Snyk categorization, we block issues from our end while raising a pull request and also before releasing to production.

“We need Snyk because we are in the banking industry with thousands of

applications. Every day, we deploy code to production, releasing almost every day except weekends, though we sometimes release on weekends for very large deployments. Anything that goes to production should not have any security vulnerabilities. Being in the banking industry and having applications used by end customers, we are dealing with end customer data. No one should steal data in any format, and with authentication, one user cannot see another user's data. Snyk is paramount and extremely important for us. Every application that goes into production must pass Snyk vulnerability scanning before it can be deployed. If you ask whether it is important, it is absolutely critical. I would rate it 10 out of 10.

“Internally, whenever a Snyk scan runs, we have created [GitHub Actions](#). Our target state is [GitHub Actions](#) everywhere. When we run the GitHub Actions, it will connect to the latest Snyk scanning through API and automatically gets all open issues, then creates a [GitHub](#) issue. First, our internal tool pulls out all Snyk security issues through the API and creates [GitHub](#) issues. We manually open a GitHub issue and give a command prompt to our AI agent. That prompt internally might work with Snyk autofix capability and gets the fixes correctly and creates a pull request. We review and check in the pull request, which is reviewed by experienced team members. This is the process we follow: create an issue based on a Snyk scan and for every issue, run a prompt so that it creates a pull request automatically with the fixes.

“We do use Snyk documentation. We internally do not have many resources because we do not want to duplicate. Snyk guide is purely open and not logged in, so we use it.

“Snyk documentation is extremely useful. Vulnerability-wise, I do not go to Snyk documentation frequently because in the current world, with my 25 plus years of experience, I used to fix many things manually before these tools existed. I need to know the intricacies of how to fix code. If you take 10 years back, there were tools and libraries which you could integrate with one or two lines, which solved the problem. With the current AI world, I do not even need that. If I get some issues, I do not even need to go to the Snyk website and read how to fix. I have an AI tool that can fix it if I ask it to. From an engineer's perspective, I still read the documentation. As a person who came from the manual world 25 years back, I still read the fix documentation. The documentation is very good, and being a general

one, I understand the SAST world, so I did not find much problem with the documentation.

“We are using Snyk, which is a SAST tool. There is a team in our organization who developed some AI agent on top of Snyk capabilities. I do not know exactly how they integrated Snyk, but our organization provides an AI agent which, if we run, automatically fixes issues and raises a pull request. In that case, we are indirectly using Snyk.

“My overall rating for Snyk is 10 out of 10..”

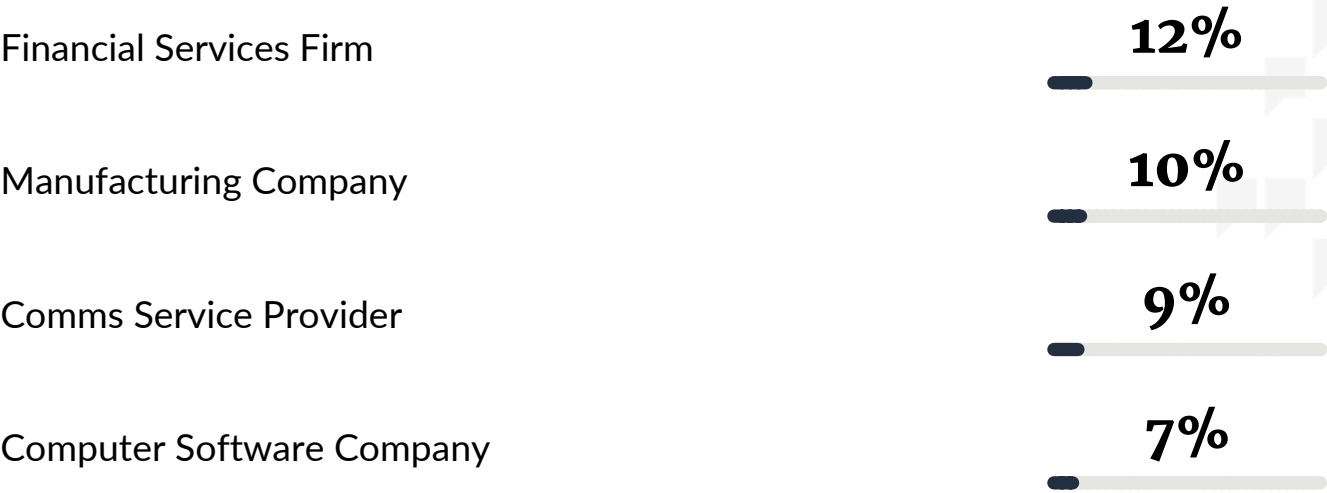
KannanPadmanabhan

Senior Software Engineering Manager at a financial services firm with 10,001+ employees

[Read full review](#) 

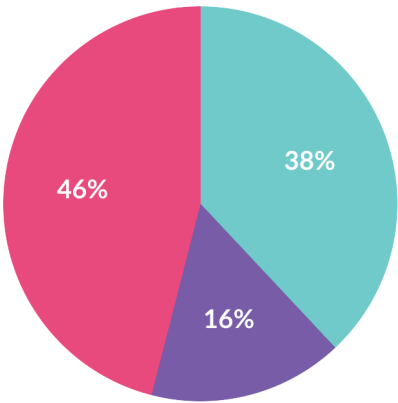
Top Industries

by visitors reading reviews

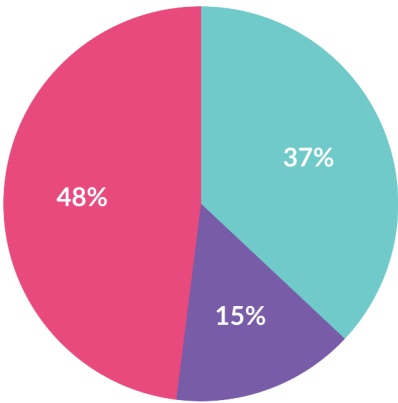


Company Size

by reviewers



by visitors reading reviews



Large Enterprise Midsized 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