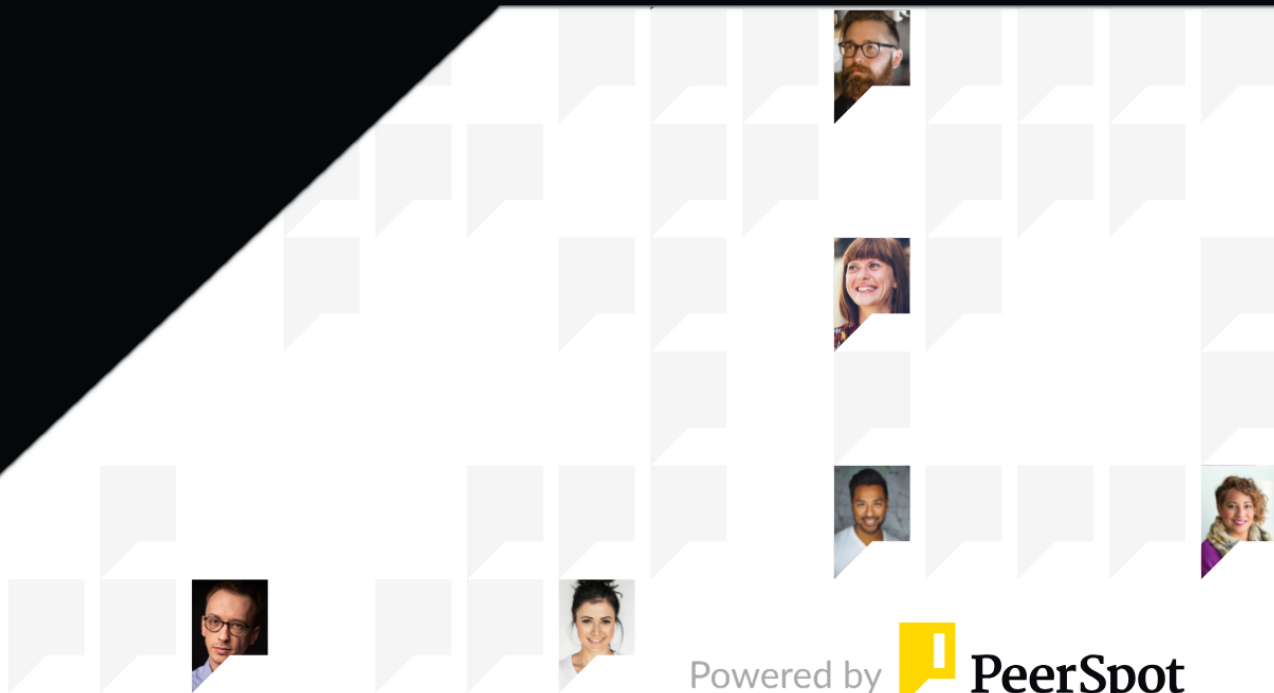


aws marketplace

Mend.io

Reviews, tips, and advice from real users



Powered by  PeerSpot

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 12

Other Solutions Considered..... 13 - 16

ROI..... 17 - 20

Use Case..... 21 - 25

Setup..... 26 - 29

Customer Service and Support..... 30 - 32

Other Advice..... 33 - 38

Trends..... 39 - 40

About PeerSpot..... 41 - 42

Product Recap



Mend.io

Mend.io Recap

Mend.io integrates seamlessly into development environments, providing open-source dependency scanning, CVE detection, and license management to enhance security and efficiency during code development.

Mend.io delivers comprehensive open-source vulnerability detection and remediation, seamlessly integrating with CI/CD workflows. It equips organizations with tools for software composition analysis and license risk detection, efficiently identifying vulnerabilities and managing policies. Mend.io supports a wide array of programming languages and deployment environments while integrating with developer tools like GitHub, Jenkins, and Azure DevOps to enhance security feedback and decision-making. Its ease of use and rapid setup boost efficiency in managing open-source dependencies and reducing vulnerabilities.

What are Mend.io's Key Features?

- Open-source dependency scanning: Efficiently scans and identifies vulnerabilities in third-party libraries.
- CVE detection: Detects and alerts on potential security risks with granularity.
- License management: Manages open-source licenses to ensure compliance and reduce legal risks.
- Integration: Works seamlessly with Visual Studio, Azure DevOps, and more.
- Fix suggestions: Provides actionable solutions to identified vulnerabilities.
- Automated policy management: Enhances security by automating policy adherence.

What Advantages Should be Considered in User Feedback?

- Development efficiency: Streamlines workflows to improve code security and quality.
- Rapid setup: Minimal time investment required, allowing immediate integration into existing processes.
- Extensive language support: Accommodates multiple programming environments, enhancing flexibility.
- Robust integration options: Compatible with top development tools, bolstering productivity.

Mend.io empowers industries such as finance, healthcare, and e-commerce by integrating robust open-source security measures within their development cycles, enhancing their ability to address vulnerabilities swiftly and maintain compliance amidst rigorous regulatory standards.

Valuable Features

Excerpts from real customer reviews on PeerSpot:



“Once we onboarded to Mend.io, we saw a drastic improvement in the way Mend.io reported the SCA findings.”



meetharoon

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



“In my opinion, it is the best because with respect to the scan coverage, it is giving basically all the components we are looking for and all the requirements we require, and compared to other tools, especially in terms of identifying and integrating into our DevSecOps and CI/CD, Mend.io is compatible, with good integration coverage across all the technologies it supports and a relatively low noise ratio with accurate issues and useful customization options.”



Verified user

Project Associate at a tech vendor with 10,001+ employees



“The home dashboard itself gives a very good analysis for Mend.io; this is not just for SCA, it is for SAST and container as well, and it gives entire analytics of how many vulnerabilities were found, how much was updated, and how much was fixed over the last three, six, and nine months.”



Sonal Moon

Product Security Architect at a computer software company with 10,001+ employees



“The features I find most valuable in Mend.io are the ease of use; it is very easy to access and integrate.”



Verified user

VP at a tech vendor with 5,001-10,000 employees



“Mend.io is very robust in terms of managing third-party dependencies.”



meetharoon

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



“Mend.io is a security tool that provides security feedback for all tests.”



SrikanthRaghavan

Principal Architect at a consultancy with 11-50 employees



“The best feature is that the Mend R&D team does their due diligence for all the vulnerabilities. In case they observe any important or critical vulnerabilities, such as the Log4j-related vulnerability, we usually get a dedicated email from our R&D team saying that this particular vulnerability has been exploited in the world, and we should definitely check our project for this and take corrective actions.”



Sonal Moon

Product Security Architect at a computer software company with 10,001+ employees

What users had to say about valuable features:

“Mend.io is very robust in terms of managing third-party dependencies. It has a built a substantial database of dependencies in their system and incorporates many open-source databases. This makes it very effective, and we find it 100% accurate in detecting vulnerabilities. It supports the largest number of languages, over 200, which is highly beneficial for us..”

meetharoon

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

[Read full review](#) 

“Mend.io is a security tool that provides security feedback for all tests.

“It handles Application Security, performing SCA SAST and container scanning.

“They completed a complete shoulder shifting for us to set up Mend.io at the enterprise level.

“We had zero workloads because Mend.io was able to handle all the lift and shift of tasks. We only needed to register the application and start using it..”

SrikanthRaghavan

Principal Architect at a consultancy with 11-50 employees

[Read full review](#) 

“What I think about Mend.io is that it is very efficient, highly efficient, and it is the best scanning tool for SCA.

Mend.io stands against other SCA solutions on AI; I would say it is on the top compared to any other tool in the market.

The continuous monitoring capabilities in Mend.io aided our organization in maintaining a secure environment; that was wonderful. We automated processes and we actually created our own centralized platform where all the feeds were ingested, and we could see the SAST, DAST, IAST, and SCA everything in one single place. So we had to do some work, but we actually did custom centralization of efforts and were able to ingest everything into our own platform, our own centralized platform..”

meetharoon

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

[Read full review](#) 

“The features in Mend.io that I have found most valuable are the scan engine, which is pretty good. Mend.io has improved the scan engine on their side, so all the vulnerabilities are having less false positives as the years go by.

“The home dashboard itself gives a very good analysis for Mend.io. This is not just for SCA; it is for SAST and container as well. It gives entire analytics of how many vulnerabilities were found, how much was updated, and how much was fixed over the last three, six, and nine months.

“We had an internal analytics, but Mend.io's analytics also gives us a fair comparison regarding how it works and how effective it was, how many vulnerabilities were found over time, and how many were fixed..”

Sonal Moon

[Read full review](#) 

Product Security Architect at a computer software company with 10,001+ employees

“The features I find most valuable in Mend.io are the ease of use; it is very easy to access and integrate.

“We have been using the automated vulnerability detection feature, and while I am aware of it, there is some delay, so we have been working with them to enhance it further.

“Mend.io's detailed dependency analysis is good, and I am looking forward to the usage of AI, especially from the perspective that not all CVE IDs are exploitable.

“The monitoring capabilities in Mend.io are good because we have integrated it with a pipeline, and overall the experience has been good.

“Mend.io's reporting tools are beneficial for my use case; from a UI perspective and generation of reports, including the SBOM, it has the flexibility and is easy to generate and share with the developer teams..”

Verified user

[Read full review](#) 

VP at a tech vendor with 5,001-10,000 employees

“The key benefit of Mend.io is that we were able to automate and integrate this tool into our CI/CD, and we can scan. Basically, it can reduce the cybersecurity risk by identifying the risk and then fixing the vulnerable open-source components before they get exploited. We can integrate them into our CI/CD, and we can identify and fix the issues. It improves the compliance with respect to not only the component but also we can look at the license management aspect, policy enforcement aspect, then updating the bill of materials, generating the SBOM, and making sure that the vulnerability information is stored and that can give a future aspect of detecting early and giving the good results. Obviously, it can reduce our cost by lowering the remediation cost by finding and fixing the issue during the early stage of our SDLC. During the development life cycle itself, we can integrate these into pipelines as part of our DevSecOps integration. It will have a capability to support all the integrations within our DevSecOps. That will give us faster results and the ability to quickly find out the vulnerabilities and then fix them so that way we can reduce the cost. Proactively, we can pick up the vulnerabilities and then fix them rather than moving to the later stage of the software development life cycle.

“With respect to the end-user perspective, we can directly integrate these into, for example, IDEs or maybe Git repositories and then CI/CD pipelines. We can automate all the dependencies. We can identify the issue and fix it, so that obviously reduces the manual effort. Based on the severity which it is giving, we can prioritize the exploitability of the vulnerability. We can understand the risk context. It will help us to focus on what matters most. That way, basically, both from the end-user perspective and as well as the business perspective, leveraging this tool definitely helps us to identify the vulnerability at the early stage of the software development life cycle and also be able to get it fixed. All the ways of development aspect as well as the business aspect, it is helping us as a tool to proactively manage vulnerability management very effectively to minimize the risk from the software supply chain..”

Verified user[Read full review](#) 

Project Associate at a tech vendor with 10,001+ employees

Other Solutions Considered

“Before Mend.io, we had a manual process. That means we were tracking all the licensees and copyrights manually. We also tried using an open-source tool to detect vulnerabilities and fix them, but it did not work very well. It was consuming a lot of time on my team..”

Verified user

[Read full review](#) 

Release Manager at a tech vendor with 501-1,000 employees

“In my opinion, there is one main competitor for Mend.io, but we are not considering it. We are happy with Mend.io. However, Snyk is another solution that I have seen many of my friends implement..”

Sonal Moon

[Read full review](#) 

Product Security Architect at a computer software company with 10,001+ employees

“We evaluated Black Duck and Snyk. We went with Mend, not because of pricing—we were willing to pay the right price for the right tool—nor for the features. It was for the ability to track all the copyrights when using an open-source dependency. That means we wanted all the copyrights for all the tools contributing to a given open-source dependency. Mend.io was the only tool that could do that..”

Verified user

[Read full review](#) 

Release Manager at a tech vendor with 501-1,000 employees

“Previously, we used different tools; I actually was involved in the decision-making process. Once we onboarded to Mend.io, we saw a drastic improvement in the way Mend.io reported the SCA findings. Many people were also using SonarQube and some other tools for their internal processes, which was not official, but when they reported, they said the other tools were reporting a lot of false positives compared to Mend.io. No one complained that this is a false positive in Mend.io; we were actually able to see if Mend.io shows there is a problem here, and we used to ask the dev teams to go inside those directories and discover, and they actually said there is a problem..”

meetharoon

[Read full review](#) 

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

“After conducting a thorough evaluation that spanned approximately three to four months, we made the decision to transition from Fortify to Synopsys Coverity for our Static Application Security Testing (SAST) needs. Coverity emerged as an ideal solution during our assessment, particularly due to its impressive ability to minimize false positives, achieving a rate of less than 5% across a range of codebases from a few thousand lines to over a million lines in our testing scenarios. This capability significantly enhanced our confidence in the tool's effectiveness and reliability for identifying vulnerabilities. However, after several years of renewals and continued use, we ultimately chose to discontinue our use of Coverity. This decision was primarily influenced by the licensing costs associated with Synopsys, which became increasingly burdensome as our organization sought to optimize expenses. Additionally, we faced integration difficulties related to our forthcoming ecosystem centralization initiatives. As we aimed to streamline our security processes and tools across various divisions, it became clear that maintaining Coverity would not align with our strategic goals. Consequently, around 2018 or 2019, we decided to adopt Checkmarx and Mend.io as our new solutions. This switch was driven by the need for tools that not only provided robust security features but also offered better integration capabilities and cost-effectiveness within our evolving infrastructure. The transition reflects our commitment to continually assess and refine our security posture, ensuring that we leverage the best tools available for safeguarding our software development efforts..”

meetharoon

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

[Read full review](#) 

“We continue to evaluate various products that offer significant benefits in terms of reducing the time required to remediate vulnerabilities and minimizing the efforts placed on developers. Our evaluation process has included several notable solutions, such as AppScan and Veracode, both of which are cloud-based options designed to enhance application security through static analysis. Additionally, we assessed CodeSonar, Contrast and Fortify, both of which provide robust capabilities for identifying security flaws and quality issues within code. In our ongoing search for optimal solutions, we also explored GitHub Advanced Security, which is currently under assessment. This tool integrates seamlessly with the GitHub ecosystem, offering unique features tailored for teams already utilizing GitHub for version control. Furthermore, we evaluated Checkmarx, a well-regarded SAST tool that has been instrumental in our security strategy; however, we have decided to decommission it as we pivot towards more integrated and cost-effective alternatives. Our thorough evaluation process reflects our commitment to adopting tools that not only improve security but also enhance developer productivity by streamlining workflows and reducing the burden of manual remediation efforts. Each product was scrutinized for its effectiveness in addressing our specific needs, including ease of integration within our existing systems, cost implications, and overall impact on our development lifecycle. As we move forward, we remain dedicated to continuously assessing new technologies that can further optimize our security posture while supporting our development teams effectively..”

meetharoon[Read full review](#) 

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

ROI

Real user quotes about their ROI:

“We are seeing a return on investment because the code quality has improved, and it improved our reaction to the kinds of incidents that are happening outside the industry..”

Verified user

[Read full review](#) 

Sr. Manager at a financial services firm with 10,001+ employees

“We have seen an ROI. We were able to find vulnerabilities. If our products were not attacked by an external entity, we consider that as an ROI, but it is difficult to put a dollar value on that..”

Sonal Moon

[Read full review](#) 

Product Security Architect at a computer software company with 10,001+ employees

“In terms of resources, we are saving 15 percent of our time when remediating issues. And for our company, there is a big financial gain because people can work on multiple projects. And most importantly, we know we are not delivering products with high CVEs, which makes it safer for our customers. .”

Verified user

[Read full review](#) 

Release Manager at a tech vendor with 501-1,000 employees

“We can see a return on investments because we have no security breaches, security costs, or GDPR issues. ROI is hard to calculate for security. You could spend time with fixes, but it's hard to say precisely how much you saved if you never have a breach. When we fix a vulnerability, we don't know what it would've cost us if it had been exploited. The return on investment is having a secure product..”

Kieran Whelan

[Read full review](#) 

Principal Security Engineer at Texthelp Ltd.

“The return on investment is there. They need to realize that there are other competitors in the space. GitHub now has GitHub Advanced Security, for example. They don't yet have parity with Mend (formerly WhiteSource), however, they're getting close. Within six months to a year, they'll be there. Their pricing is also quite a bit less. At some point, Mend (formerly WhiteSource) is going to have a pricing problem.

We've seen ROI in terms of the removal of manual processes and accelerated delivery. We were spending a lot of time having to try and track OSS libraries manually. That was frankly a hopeless exercise. In that sense, removing that bureaucracy removed costs from our organization and sped up delivery.

There's also a risk avoidance aspect to Mend (formerly WhiteSource). If there are CVEs against any of these components that we don't know about, it's very hard with manual records to go back and guarantee that all these components are clean. We needed a powerful tool to do it and so the risk avoidance definitely does reduce our costs simply in terms of compliance..”

Jeffrey Harker

System Manager of Cloud Engineering at Common Spirit

[Read full review](#) 

“Mend.io has demonstrated a strong return on investment (ROI) for our organization by effectively minimizing vulnerabilities and fostering a culture of security awareness among our development teams. The solution excels in Software Composition Analysis (SCA) and container management, emphasizing vulnerability reduction while enhancing our organizational culture, all of which contribute to delivering optimal ROI. One of the most significant impacts Mend.io has had on our operations is its ability to automate the identification and remediation of open-source vulnerabilities. This automation has led to a substantial reduction in the time our developers spend addressing security issues, enabling them to focus more on innovation and less on remediation. In fact, we have observed a notable decrease in the mean time to resolution for vulnerabilities, which translates directly into cost savings and improved productivity. Additionally, Mend.io's integration capabilities with our existing development workflows have streamlined processes across teams. By embedding security checks into our CI/CD pipelines, we have accelerated our application delivery timelines while ensuring that security is prioritized from the outset. This proactive approach not only mitigates risks but also enhances our ability to meet project deadlines and deliver safer products to our customers. Furthermore, the tool's comprehensive reporting features have provided us with valuable insights into our security posture, allowing us to make informed decisions about risk management and compliance. The visibility it offers into our software supply chain has empowered us to take a more strategic approach to security, aligning with industry best practices and regulatory requirements. From a financial perspective, the cost savings associated with reduced manual processes and faster remediation times have significantly contributed to our ROI. Organizations using Mend.io have reported savings of up to 15% in time spent on vulnerability management, which can lead to substantial financial gains over time. As we continue to leverage Mend.io's capabilities, we anticipate further enhancements in ROI through improved security metrics and operational efficiencies. In my personal opinion, Mend.io not only serves as an effective tool for managing software vulnerabilities but also plays a crucial role in cultivating a security-focused culture within our organization. Its ability to deliver measurable results in terms of both cost savings and enhanced productivity underscores its value as a strategic investment in our application security efforts..”

Use Case

“I am using it for Software Composition Analysis, mainly for third-party open-source library security perspective and the license compliance perspective..”

Verified user

VP at a tech vendor with 5,001-10,000 employees

[Read full review](#) 

“Mend is a SaaS solution we use to make open source libraries for our products. It covers license usage, license type, and CVE vulnerabilities. We use Mend at our Belfast office, but a subsidiary in Norway also has access to it. There are 67 users at our company. About four are admins, and the rest are developers. .”

Kieran Whelan

Principal Security Engineer at Texthelp Ltd.

[Read full review](#) 

“We have two primary use cases. One use case is to find the vulnerabilities related to the open-source libraries that are included in multiple products in our company.

The second use case is to find out whether the licenses associated are for general use or not, or whether there are any license-related restrictions. Sometimes, when you use open-source components, depending on the type of licenses, they may be applicable only for internal use. We use it to check whether we are violating any licensing or not. .”

Sonal Moon

Product Security Architect at a computer software company with 10,001+ employees

[Read full review](#) 

“Mend.io is integrated into our CI/CD processes. Our primary tool for CI/CD is Concourse CI, where all development teams incorporate Mend into their pipelines. In addition to Concourse CI, some dozens of our Dev teams utilize Jenkins, GoCD, and TeamCity, along with integrations for Azure DevOps and AWS Code pipelines. Our environment generally features a variety of tools from the GitHub ecosystem and supports several programming languages tailored to specific use cases..”

meetharoon

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

[Read full review](#) 

“I have been using Mend.io and no longer work for that company after leaving a few months back. Mend.io has been used for probably three or four years and it was the best tool that we actually replaced. It was the best tool I ever saw for all the dependencies and all those things.

Everything that has to do with dependencies and third parties was ingested through Mend.io; we used the SaaS tool for a different purpose and then we used Mend.io for all dependencies.

We have been using some capabilities of Mend.io, particularly when AI started; we wanted to utilize some of the AI features, but AI is a gray area. If you want to use it specifically for AI, then that is something every organization must think about how much they should automate the processes. Other than AI, I think the automation is wonderful..”

meetharoon

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

[Read full review](#) 

“We are using Mend.io for open-source component scanning mainly, all third-party open-source components. This is especially for the software composition analysis. We do have a large number of supply chain-related vulnerabilities from the AppSec aspect. Using Mend.io, we scan all the dependency risk, and then we are able to understand the outdated packages. We are able to get the CVEs with respect to the open-source components. According to that, we will apply updating the packages to the latest patch. Then we clear all the dependency checks and identify all the libraries to which component is communicating to which component, whether we have a direct dependency or a transitive dependency. Then we update the software bill of materials for the vulnerability. The main purpose of using Mend.io is for the software supply chain security to identify and remediate the vulnerabilities which come across the open-source software components, especially dependency checks.

“In my opinion, it is the best because with respect to the scan coverage. It is giving basically all the components whatever we are looking for and all the requirements we basically required. Comparatively to other tools, especially in terms of identifying and integrating into our DevSecOps primarily into our security, Mend.io is compatible with respect to integrating with our CI/CD, and then using that, we will be able to detect and fix the vulnerabilities. The coverage of integration is good across all the technologies it is supporting. In terms of noise ratio, comparatively it is less and gives a good, accurate number of issues. There are some gaps with respect to giving an exact vulnerability. However, we were doing some tuning of the tool with respect to helping to understand basically what we are expecting to scan, then what could be the output. In that aspect, the tool also has the option to tune the tool, and we can customize what our requirement is, and based on that, we can pull the scan. That is good.

“We were able to integrate with our CI/CD pipelines. That is totally automated with respect to scan as well as updating the remediation.

“At this moment, I would say Mend.io is working based on our requirements. But in future, if we start exploring more and moving towards the AI side, AI technologies, and then obviously the threats based on the vulnerabilities, the vulnerabilities which we identified in the past and the same vulnerability or CVE is

repeating in the future, then how the data is analyzed by the tool and how it is giving the threat intelligence reports. That is more towards the AI apps. Obviously we need to look for that because at this moment we are not using for that purpose. But we need to explore that analytics part, how much it is capable of in terms of having the correct data and how much the capability the tool has so that it can give the threat intelligence reports, looking at the previous past data to get the results driven for the future requirements. We need to explore that. At this moment, without experimenting, I could not say whether this tool will be good or bad, but I am hoping this could support the analytics as well..”

Verified user[Read full review](#) 

Project Associate at a tech vendor with 10,001+ employees

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 process for Mend.io has improved; it is similar to a one CLI agent now. Earlier there were three different agents, and now there are just certain limited commands you need to run for each type of scan, and then you are good to go..”

Sonal Moon

[Read full review](#) 

Product Security Architect at a computer software company with 10,001+ employees

“I never had an opportunity to be involved because everything was proactive from Mend.io's perspective. They provide faster feedback, and whenever something fails, they proactively fix it. I would rate it nine out of 10..”

SrikanthRaghavan

[Read full review](#) 

Principal Architect at a consultancy with 11-50 employees

“It is very simple to set up Mend.io, even for developers who had no experience and no exposure to tools in Mend.io; we simply provided some straightforward instructions. We had our own internal Wiki and we wrote those instructions on how to onboard; it was pretty straightforward.

I would say it was the easiest tool to onboard..”

meetharoon

[Read full review](#) 

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

“It is a SaaS solution. I was not involved in its deployment. It was already in the company for six months when I got my hands on it.

In terms of maintenance, we just need to check which users have left the organization so that we can maintain the number of users under the license that we have purchased. That is a small thing required on our side even though we have SSO integrated..”

Sonal Moon

[Read full review](#) 

Product Security Architect at a computer software company with 10,001+ employees

“The setup was very straightforward. It took only a few minutes to be able to scan the first project. Because we had 40 or 50 projects to scan, it took about a week to set up everything.

The deployment was done by me with some help from IT.

Because we are using the SaaS solution, we don't have to upgrade the main tools. Regarding the Unified Agent, we try to upgrade a few times a year so that we are using the latest version. Overall, the maintenance is very low. We don't spend much time on it..”

Verified user

[Read full review](#) 

Release Manager at a tech vendor with 501-1,000 employees

“Setting up Mend.io was a very straightforward process for our organization, primarily because the integration with GitHub required minimal effort. Developers simply needed to integrate Mend.io into their CI-CD pipelines they use, which facilitated seamless access to our repositories. I had created technical artifacts that explains the workflows and integrations processes. Additionally, I created a standardized templated model that made it much easier to adopt. This involved additional steps and configurations to align with our specific workflows and requirements. However, we have comprehensive documentation and handholding available to assist our developers through this process, ensuring that they have the necessary guidance to navigate any challenges that may arise.

Our primary CI/CD tool is Concourse CI, and all development teams have successfully integrated Mend.io into their respective pipelines. This integration has proven beneficial across various teams, as it allows for automated vulnerability scanning during the build process, significantly enhancing our security posture. Additionally, several of our development teams utilize other tools like Jenkins, GoCD, and TeamCity, along with integrations for Azure DevOps and AWS CodePipeline. The versatility of Mend.io in adapting to these different environments has further underscored its value.

Overall, the setup experience with Mend.io has been characterized by its user-friendly interface and effective integration capabilities. The ability to quickly onboard the tool into our existing workflows has enabled us to enhance our development processes without significant overhead or disruption..”

meetharoon

[Read full review](#) 

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

Customer Service and Support

“Mend.io offers excellent customer service. They prioritize providing the best experience to large organizations like ours, belonging to the Fortune 100. On a scale of one to ten, they rate around eight to nine for customer service..”

meetharoon

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

[Read full review](#) 

“All levels of their support have very good technical knowledge. They know their tool better than us, so when we cannot find a solution, they give us that in 15 minutes. I would rate them a 10 out of 10..”

Sonal Moon

Product Security Architect at a computer software company with 10,001+ employees

[Read full review](#) 

“Regarding support, the people who were involved in the commercial side were the direct point of contact with Mend.io, but my understanding is Mend.io provides pretty good support. I did not hear any complaints from those teams that Mend.io is slow or the support is not good; I did not hear anything of that sort in my almost three or four years..”

meetharoon

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

[Read full review](#) 

“The support is great but I haven't had to use them in a long time. But it's very efficient. I also have a nice customer support manager, so I know if I have an urgent ticket to open, I open it through the main support portal and then I can contact my CSM to ask him to work with me. A few hours or a day later, someone is working on my ticket..”

Verified user

[Read full review](#) 

Release Manager at a tech vendor with 501-1,000 employees

“When it comes to technical support, I would rate them a nine; I could give ten, but just to have this response fair, I will give them nine. Their technical support is quite knowledgeable enough to answer questions.

“The response time from technical support is good as long as you define the criticality. Critical tickets are responded to within an hour..”

Sonal Moon

[Read full review](#) 

Product Security Architect at a computer software company with 10,001+ employees

“I rate Mend's support a nine out of ten. On the CVE main page, Mend points out the vulnerability and directs us to the remediation. If we're having a problem fixing it, they have a highly responsive help desk that we utilize quite a lot.

The support is great. It's highly responsive. If we open a ticket, we get a call in one or two days. Their chat option is excellent. When we look for more information, we always get a timely response. For example, when we faced a Log4j issue, they posted a lot of information and alerted us to a vulnerability in the library without us having to look at the tool. .”

Kieran Whelan

Principal Security Engineer at Texthelp Ltd.

[Read full review](#) 

Other Advice

“I am still using Mend.io.

“I am not sure about the process for purchasing that solution through the [AWS](#) marketplace or directly from Mend.io.

“I cannot take too much time for questions about Mend.io to update my previous review.

“I will continue with Mend.io because I plan to use additional tools, but I am not going to replace Mend.io.

“I rate Mend.io an eight out of ten..”

Verified user

VP at a tech vendor with 5,001-10,000 employees

[Read full review](#) 

“In terms of threat intelligence, at this moment, whatever the bill of materials we are giving, based on that, actually, with respect to enrichment, for example, looking at the CVE database and looking at the National Vulnerability Database, then some CVSS related information, that way basically it is giving us some vulnerabilities. But with respect to more on threat intelligence perspective, we also need to understand, it is important to understand that Mend.io is not a dedicated threat intelligence platform. If you look at the Microsoft Defender, maybe CrowdStrike intelligence or some other tools, maybe those are actually really threat intelligence platforms. Whereas Mend.io is not a really threat intelligence platform. But instead, we need to see how we can consume the vulnerability intelligence to improve our software supply chain security based on our decision so that we can leverage the tool. To conclude, the strengths of Mend.io that can give the threat intelligence, especially looking at the CVE database, looking at the National Vulnerability Database, then EPSS, for example, Exploit Prediction Scoring System, CVSS scoring system. Based on these, actually it is giving us the threats and as well as giving us the report. But really, we cannot completely say it is purely, at this moment we do have a threat intelligence capabilities, but we need to explore more on that aspect. I would rate this review as a ten overall..”

Verified user[Read full review](#) 

Project Associate at a tech vendor with 10,001+ employees

“I am still working with Mend.io, and I am using it.

“Regarding scanning in Mend.io for [SAST](#), I think that would be scanning, not monitoring. As I mentioned, Mend.io migrated to a new CLI version, which is pretty good. As the years go by, they have one CLI for all three scans, and Mend.io keeps updating that CLI on their side.

“The reporting tools in Mend.io, specifically the executive report that PDF report,

is a good part to show management, whereas for technical teams, I think CSV reports should be sufficient.

“The initial setup process for Mend.io has improved; it is similar to a one CLI agent now. Earlier there were three different agents, and now there are just certain limited commands you need to run for each type of scan, and then you are good to go.

“My overall review rating for Mend.io is nine..”

Sonal Moon

Product Security Architect at a computer software company with 10,001+ employees

[Read full review](#) 

“Being in the industry of security plus AI, I actually specialize in AI and have written a few books on AI available on Amazon, so I am very cautious about AI, especially anything that includes AI, particularly security tools.

As for AI and other features, AI is a gray area and no tool in the industry is anything good in AI currently. They are evolving and it will probably take five to maybe ten years to be very good in AI. AI is an upcoming area; it is not even stabilized and is an evolutionary area. So anything we want to use, whether it is SCA, [SAST](#), DAST, IAST, or any tool, we have to be very careful with AI.

The documentation is huge and awesome; it's huge.

Since it is a huge Wikipedia, some links might be a little outdated; what they do is point to the new location, and sometimes that new location becomes confusing because it auto-redirects. If we had to refer to some old documentation and we want to just for cross-references to what we had done, then the old links are not available because it redirects to the new location. I think that's the usual case with any other tool because even Synopsys had a similar thing where they had huge documentation, and whatever updates were there, they used to redirect those pages.

Overall, I cannot give a 10 to any tool in the market because no tool would be perfect. Except for the AI part, which I am very sensitive to in any tool in the market, otherwise, I would give a rating of nine; it is a very good tool to use. I have provided a rating of 9 for this review..”

meetharoon

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

[Read full review](#) 

“Mend.io is highly recommended for organizations looking to implement Software Composition Analysis (SCA), as it stands out as a top choice with a 100% accuracy

rate in vulnerability detection in our case and experience being among the largest scale of implementation; although we understand every customer scenario and experience may vary. While no tool can claim to be flawless, for us Mend.io has consistently delivered reliable results, and I would rate the solution at 9/10. This rating reflects my belief in its effectiveness while acknowledging that there is always room for continuous development and improvement in any software solution..”

Moreover, the incorporation of artificial intelligence (AI) into code security tools like Mend.io is still in its early stages. Although many vendors tout advanced AI functionalities, it may take several more years for these features to reach a level of maturity and stability that organizations can fully rely on. We recognize the practical realities involved within the software development lifecycle (SDLC) and the cultural dynamics within development teams, which often influence how effectively these AI features can be integrated and utilized. As organizations consider adopting Mend.io, it's essential to keep in mind that while it offers powerful capabilities for SCA, ongoing advancements in technology will continue to shape the landscape of code security tools. Companies should remain open to evolving their strategies as new features and improvements become available. Additionally, engaging with the vendor for insights into their roadmap can provide valuable context on how future developments may enhance the tool's effectiveness. In a nutshell, in my opinion, Mend.io is a strong contender for those seeking an effective SCA solution, particularly given its high accuracy and user-friendly setup. However, organizations should also be mindful of the evolving nature of AI in this space and remain adaptable to changes that could enhance their security posture over time. If anyone has a need of an experienced and professional consultation, they can reach out to me.

meetharoon

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

[Read full review](#) 

“Mend SCA is better than Mend SAST. They are a market leader in SCA. The adoption of Mend SCA and the scanning of Mend SCA are pretty good. It is one of the best solutions for SCA. It was already deployed for at least six months before I got this tool. At one point, I saw WhiteSource's name on the Microsoft website as a critical solution for open-source scanning, which made me think that this solution must be good if Microsoft mentioned it on its website.

Its adoption was very slow in the beginning. Three years ago, there was no awareness of using this solution, so we had to tell the team about what the solution is for, what are its advantages, how it impacts their product, and so on. The adoption is good now, and people know exactly what it is being used for. They know the types of vulnerabilities that are there. They know the types of features that are there. Earlier, they used to go through me for any support program, but now they are directly raising tickets depending on the priority of the ticket and then directly communicating with my support representative to fix them. The initial one and a half years were difficult.

We are also using Mend SAST. They have a variety of different application security solutions in addition to SCA. These solutions are complementary. When you use solutions from different vendors, more diversity can lead to problems. When you have a Mend solution for SCA and a Mend solution for SAST, they are complementary, so the results of those scans would be far more helpful than having different vendors at each and every level. Diversification is good to a certain extent, but if you diversify too much, you might get a lot of false positives.

Overall, I would rate Mend SCA a 10 out of 10. It is definitely one of the best ones in the market..”

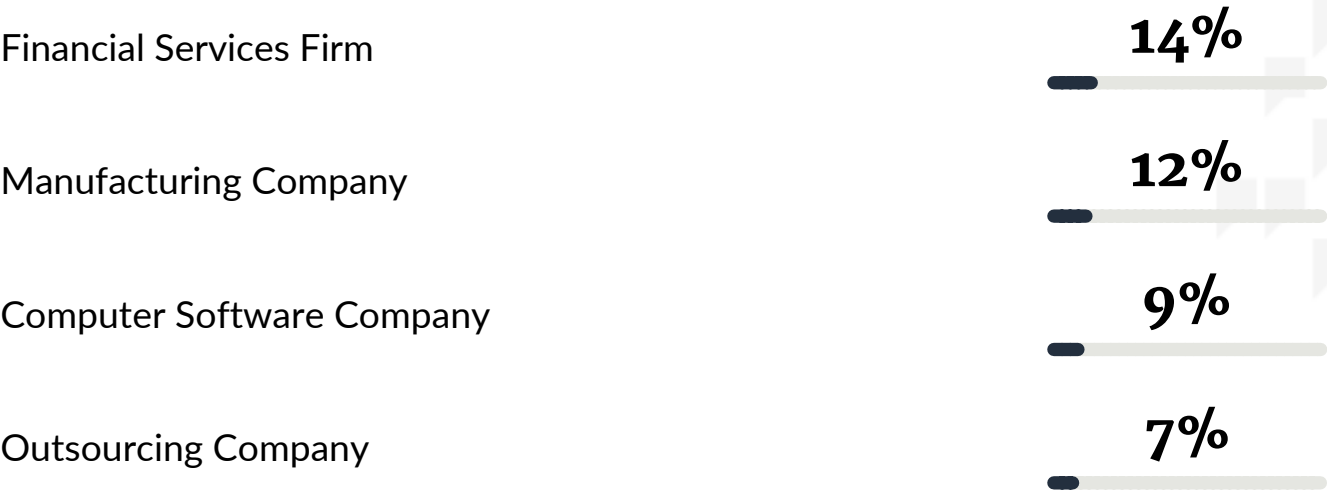
Sonal Moon

Product Security Architect at a computer software company with 10,001+ employees

[Read full review](#) 

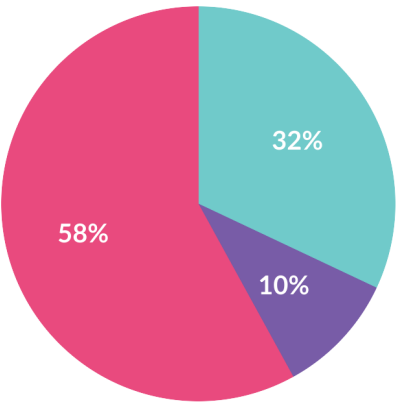
Top Industries

by visitors reading reviews



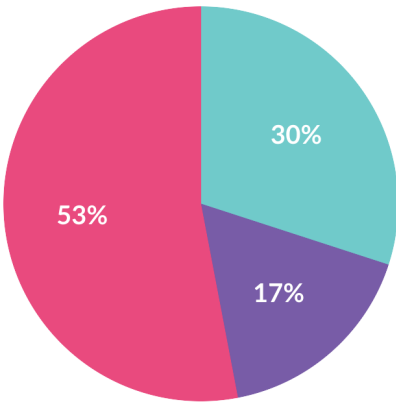
Company Size

by reviewers



Company Size

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