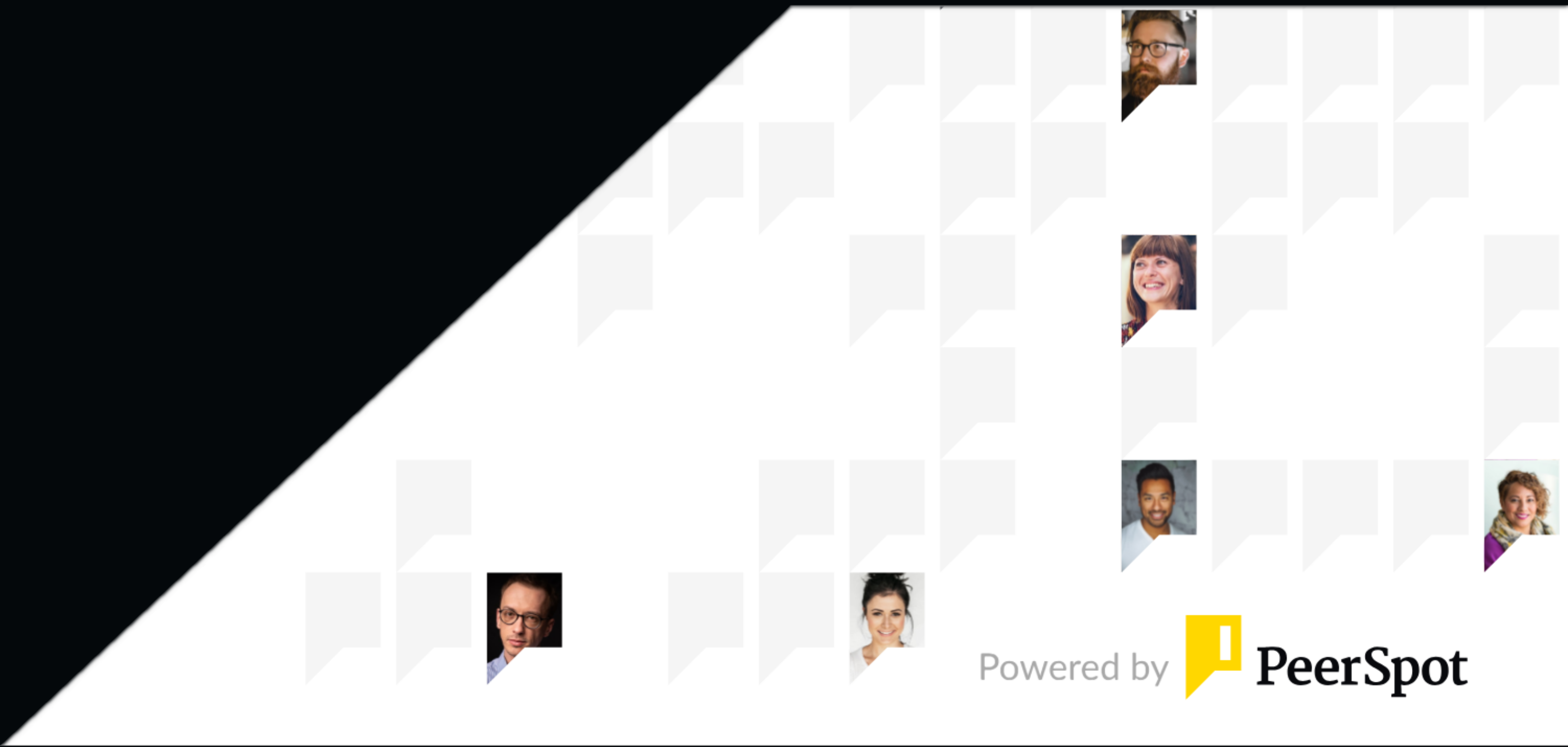
aws marketplace

Mend.io

Reviews, tips, and advice from real users



Powered by PeerSpot

Contents

Product Recap

Mend.io

Mend.io Recap

Mend.io is a software composition analysis tool that secures what developers create. The solution provides an automated reduction of the software attack surface, reduces developer burdens, and accelerates app delivery. Mend.io provides open-source analysis with its in-house and other multiple sources of software vulnerabilities. In addition, the solution offers license and policy violation alerts, has great pipeline integration, and, since it is a SaaS (software as a service), it doesn't require you to physically maintain servers or data centers for any implementation. Not only does Mend.io reduce enterprise application security risk, it also helps developers meet deadlines faster.

Mend.io Features

Mend.io has many valuable key features. Some of the most useful ones include:

- Vulnerability analysis
- Automated remediation
- Seamless integration
- Business prioritization
- Limitless scalability
- Intuitive interface
- Language support
- Integration
- Continuous monitoring
- Remediation suggestions
- Customization

Mend.io Benefits

There are many benefits to implementing Mend.io. Some of the biggest advantages the solution offers include:

- **Easy to use:** The Mend.io platform is very user-friendly and easy to set up.
- **Third-party libraries:** The solution eases the process of keeping track of all the used third-party dependencies within a product. It not only scans for the pure occurrence (also transitively) but also takes care of licenses and vulnerabilities.
- **Static code analysis:** With Mend.io's static code analysis, you can quickly identify security weaknesses in custom code across desktop, web, and mobile applications.
- **Broad support:** Mend.io provides 27 different programming languages and various programming frameworks.
- **Easy integration:** Mend.io makes integration very easy with existing DevOps

environments and CI/CD pipelines so developers don’t need to manually configure or trigger the scan.

- **Ultra-fast scanning engine:** The solution’s scanning engine generates results up to ten times faster than legacy SAST solutions.
- **Unified developer experience:** Mend.io has a unified developer experience inside the code repository that shows side-by-side security alerts and remediation suggestions for custom code and open-source code.

Reviews from Real Users

Below are some reviews and helpful feedback written by PeerSpot users currently using the Mend.io solution.

Jeffrey H., System Manager of Cloud Engineering at Common Spirit, says, “Finding vulnerabilities is pretty easy. Mend.io (formerly WhiteSource) does a great job of that and we had quite a few when we first put this in place. Mend.io does a very good job of finding the open-source, checking the versions, and making sure they're secure. They notify us of critical high, medium, and low impacts, and if anything is wrong. We find the product very easy to use and we use it as a core part of our strategy for scanning product code moving toward release.”

PeerSpot reviewer Ben D., Head of Software Engineering at a legal firm, mentions, “The way WhiteSource scans the code is great. It’s easy to identify and remediate open source vulnerabilities using this solution. WhiteSource helped reduce our mean time to resolution since we adopted the product. In terms of integration, it's pretty easy.”

An IT Service Manager at a wholesaler/distributor comments, “Mend.io provides threat detection and an excellent UI in a highly stable solution, with outstanding technical support.”

Another reviewer, Kevin D., Intramural OfficialIntramural at Northeastern University, states, "The vulnerability analysis is the best aspect of the solution."

Valuable Features

Excerpts from real customer reviews on PeerSpot:

✓ “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 Pitney Bowes Inc.

✓ “What is very nice is that the product is very easy to set up. When you want to implement Mend.io, it just takes a few minutes to create your organization, create your products, and scan them. It's really convenient to have Mend scanning your products in less than one hour.”

Verified user

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

✓ “There are multiple different integrations there. We use Mend for CI/CD that goes through Azure as well. It works seamlessly. We never have any issues with it.”

Kieran Whelan

Principal Security Engineer at Texthelp Ltd.

✓ “Mend has reduced our open-source software vulnerabilities and helped us remediate issues quickly. My company's policy is to ensure that vulnerabilities are fixed before it gets to production.”

Verified user

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

✓ “We set the solution up and enabled it and we had everything running pretty quickly.”

Jeffrey Harker

System Manager of Cloud Engineering at Common Spirit

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's integration with developer workflows is a massive part of our work. We use Visual Studio, and it integrates flawlessly with that. There is also a Chrome extension called Mend Advise that lets our team check libraries for vulnerabilities before they download and use them. It's a useful product.

There are multiple different integrations there. We use Mend for CI/CD that goes through Azure as well. It works seamlessly. We never have any issues with it..”

Kieran Whelan

Principal Security Engineer at Texthelp Ltd.

Read full review

“The GitHub integration is one feature we use heavily. It has helped us identify and remedy vulnerabilities. Mend is also easy to use. Once it's configured, it's seamless for the development community. It's clearing issues for them so that they can see the problems and how to fix them.

We have already integrated Mend with the developers' workflows, including the IDE repository and CI/CD pipelines. Our developers use these IDE keys because it only supported one of the IDEs when we started: IntelliJ IDEA. They have improved and added support for multiple IDEs. We've integrated with more than 50,000 repositories. I think it's nearly 60,000..”

Verified user
Sr. Manager at a financial services firm 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 is very nice is that the product is very easy to set up. When you want to implement Mend.io, it just takes a few minutes to create your organization, create your products, and scan them. It's really convenient to have Mend scanning your products in less than one hour.

They also have a lot of integrations with different Git providers, like GitHub, GitLab, and Bitbucket.

It also has a nice tool we can use with the command line. We have continuous integration, and with the command line, we can scan everything without using the user interface. The command line is great. They have a lot of tools and plug-ins for your IDEs to automate scans. Using the command line, the Unified Agent, you can do a bunch of automated operations.

Thanks to the integration we put in place, it's super easy to identify and remediate open-source vulnerabilities, because on every commit of the software we trigger a Mend.io scan. We know, within five minutes, if the new version of the product is impacted by a CVE. If it is, we receive an email, an alert, so that the developers can fix the code. .”

Verified user

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

Read full review

“I am the organizational deployment administrator for this tool, and I, along with other users in our company, especially the security team, appreciate the solution for several reasons. The UI is excellent, and scanning for security threats fits well into our workflow.The solution is also highly valuable to our Intellectual Property Councils, because as a company that uses open-source software, we need to be aware of intellectual properties, code violations, and adherence to our regulations when we include such software. There are, of course, areas for improvement, but it has become mandatory within our organization to run scans using Mend as part of our workflows.

We don't always use WhiteSource SmartFix, and that depends on the recommendations provided by the solution's analysis. On occasion, we have challenged those recommendations, so for us, the software is not entirely a decision-making tool but a tool that assists us in making decisions. Therefore, there is still a human component in the process, and there is always an admin or approver to accept or reject the recommendation. There have been instances where smart fixes were challenged due to a lack of compatibility with project requirements. For example, the solution recommends a version of PostgreSQL, but the decision is made on the product level to go with a different version because it has better integration with the specific product requirements. However, I would say that SmartFix increases our decision-making effectiveness and successfully alerts us. As a leading lighting company, some product decisions must adhere to strict requirements, which require human involvement in the decision-making process.

Initially, the product didn't save us time but required us to spend more time. Many of our processes require a manual component, so we can't entirely rely on automated processes. Therefore, when we run Mend scans on our projects, around 60% of the software development life cycle is sped up, while the remaining 40% requires human intervention. Per our IP Councils, automation does not help us beyond a certain point, and manual intervention is required. If 60% of a project can be streamlined via automation, that certainly saves us time.

I would say that Mend certainly helps us detect and reduce vulnerabilities. We bring in the solution at the very beginning of a project, so we build early and often and detect vulnerabilities early. This is a significant contributor to our projects' success.

Integration using the unified agent and other methodologies has been at the forefront of our deployment. The plugins have been merged into the unified agent approach. The integration methodologies have worked wonders for our CICD pipelines and workflows, and each project team can decide whether to run scans pre or post-build. .”

Verified user

IT Service Manager at a wholesaler/distributor with 51-200 employees

Read full review

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

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

Read full review

“The solution was there when I joined. During the license renewal process, we looked at other solutions, but none of them offered the level of integration we need. We will look at other solutions before the next renewal in December. The main factors are pricing and integration. Mend is the best solution for now..”

Kieran Whelan

Principal Security Engineer at Texthelp Ltd.

Read full review

“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

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

Read full review ↗

“We had other solutions, like SAST scanning and Black Duck, but nothing offered this level of detail. The previous solutions were reactive and required a lot of manual work, whereas Mend proactively identifies vulnerabilities. The code is scanned immediately once it goes into the repository.

Mend has the ability to control the release using the same data going into production or our test environments. That is what sets it apart from other tools. Other tools are emerging with similar capabilities, but when we picked it, it was one of the only tools that had the features we need. .”

Verified user

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

Read full review ↗

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

Read full review

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

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

Read full review

“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

Product Security Architect at Pitney Bowes Inc.

Read full review

“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

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

Read full review

“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

Principal Security Engineer at Texthelp Ltd.

Read full review

“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..”

meetharoon

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

Read full review ↗

Use Case

“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 Pitney Bowes Inc.

Read full review ↗

"We use open-source libraries or software in projects across our company. We conducted an internal study regarding the legalities, security, vulnerabilities, and license compliance, which is when we decided to implement and deploy Mend. It automates the software composition analysis, which is vital when we want to use third-party and open-source software.

We have a total of around 1000 projects running in Mend; some of those are being trialed and may be withdrawn, and others will go on to the production stage. We have between 300 and 400 end users, primarily integrators and fewer admins and approvers.."

Verified user

IT Service Manager at a wholesaler/distributor with 51-200 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

“Earlier, Mend was used as a tool behind the scenes for periodic vulnerability checks. It was more reactive. We only began exploring its full potential once we started integrating it with GitHub because that helped us control, and manage the process. It centrally controls all the code going into production. We have built-in rules against the license policy vulnerabilities. We don't allow code to go to production if it hasn't met those criteria.

Mend has a SaaS environment where all the data is stored, but we do all scanning and remediation work on a component that scans and identifies dependencies. It can be deployed on-prem or on the cloud using their containers. Then, it talks to the SaaS platform for the final identification of vulnerabilities and license composition.

They have also devised a smart tree containing other tools we plan to evaluate. We haven't used their SAST solution yet, but we're considering it and comparing it to the other SAST tool we use. We use Mend Renovate, which was previously an open-source product. The merge confidence feature is part of Renovate feature. Most of our people are focusing on vulnerability remediation. It gives an excellent idea about how we can move forward with a change.

Mend is deployed on the AWS cloud, and we have multi-region enabled. It is deployed active-active in both regions. This is a heavy implementation. The company has a centralized GitHub platform where every developer and team manages their code. There are more than 5,000 users. Changes appear in the report, and actions are happening internally based on that. They may not all be going to the Mend platform to see these results. There are only maybe 5,000 active commits happening monthly. The number of records per project enabled for our company is nearly 60,000. .”

Verified user

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

Read full review

“We use Mend especially for code analysis. I work in the application security part of my company. Developers will build and push the code to the GitHub repository. We have a build server that pulls in the code, and we are using Jenkins to automate that to do the DevOps stuff.

Once the code is built, we create a product for that particular version on Mend. We are currently working with three different versions for our particular product. We have the products created on Mend via White Source, which has a configuration file and a back file that runs. The configuration files basically tell what parameters to use, which server URL to use, which files to ignore, and which files to use.

For example, if I just have to do Python, I can make changes in the configuration files in Excel to include just .py files and exclude all of the files. If I have to do Python and C++, I can make changes in the configuration file itself to make .py, .C++ and exclude all of those. Once that configuration file is ready, then we run a White Source back file that just connects to the server, contacts the configuration file as well, does the scan on all the files that are there in the project, the project being for, and then pushes it to Mend, our Mend page.

On our Mend page, once we go into the product page of it, we can see what libraries have been used by us and what have some vulnerabilities. We also can set policies on Mend. We set some policies for our organization to accept and reject. For each product, we also get the policy violations that the libraries go through and any new versions for any new libraries that are available on that library's parent page - the parent page being the official developers of the library. We can get the new versions as well. We get the licenses we use with the library, and most importantly, we get vulnerability alerts regarding every library we use in our code.

Once the code is pulled, scanned, and pushed, we get the UI. We go to the library alerts. Once we go to the library alerts, we can see the different severities and the different libraries with vulnerabilities. We normally just sort according to higher severity first and go down to lower severity. We check what can be ignored or what is acceptable and what cannot be ignored, and what is of high priority. Ones that are a high priority, we flag and create a ticket on JIRA. That's our platform for collaboration.

Once we create a ticket for JIRA, the developers can see it, the QA team can see it, and they will go through that as well. They can tell if the update or the upgrade of the library is possible or not. They'll check its compatibility and see if it's actually doable or not. If it's not doable, they'll just tell us it's not doable, and probably our next version of the application will have the changes - not this one. We term that as acceptable or within our domains of acceptance. However, daily, if a JIRA ticket is created, the developers get back to us saying yes or no. Mostly they can say yes to changing the library to upgrade the library. If it's upgraded, they upgrade it to the next version. We scan it again. We do a weekly scan. We'll just check the next week if that particular liability is upgraded and the vulnerability has been remediated..”

Kevin Dsouza
Intramural OfficialIntramural at Northeastern University

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.

“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

Principal Architect at a consultancy with 11-50 employees

Read full review

“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

Product Security Architect at Pitney Bowes Inc.

Read full review

“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

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

Read full review

“The deployment was mixed; there's always a window in which we are required to adapt to a tool. This solution isn't an out-of-the-box kind of model. There was some fine-tuning involved in the deployment according to our needs and specific projects, which is expected but somewhat challenging nonetheless.

The key staff involved in the deployment included me as the deployment manager, a customer success manager from Mend, a leading member of our IP Council, and the security advisers for each product. Once the deployment strategy is decided, the IP Council and security team take a back seat, and I work closely with the product architects moving forward. Deployment, fine-tuning, and getting the scans up and running takes two to two and a half days maximum per product. Ultimately, five or six key staff are involved in the solution's deployment, configuration, and maintenance. .”

Verified user

IT Service Manager at a wholesaler/distributor with 51-200 employees

Read full review

“I am the product owner of Mend at this company, so I was responsible for setting it up and the GitHub integration process. The initial setup was straightforward, but we had to do a few steps to meet the company requirements. For example, we need to enable it through the proxy and allow it to reach external registries.

We needed to configure it to go through that path and then enable and deploy the necessary package managers. That took a little work in the beginning, but everything was good once that was all figured out.

We have a team of three engineers supporting it, but they're working on this solution full-time. We get releases every other week, so we need to ensure the enrollment is up to date. That deployment doesn't take much time because we build our dock images, and we need to enable multiple package managers. They give us the docker file that we build based on our needs.

It takes a day to deploy all these components. We mainly need additional engineers to support our user community, providing answers or clarifications. Otherwise, it's just one person maybe supporting the platform.

Mend ensured the correct data version is deployed. Other than that, it's the normal maintenance of supporting our end users. They may have questions about some fixes or suspected false positives, but we have very few false positives. .”

Verified user

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

Read full review

“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 Pitney Bowes Inc.

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

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

Read full review

“I'm delighted with the technical support, especially as someone involved in the deployment. Technical support has been highly responsive to bugs or errors, helping us mitigate or fix them quickly. It was easy to interpret their technical guidance, which made my job much more manageable. I'm very satisfied and would rate them highly..”

Verified user

IT Service Manager at a wholesaler/distributor with 51-200 employees

Read full review

“I rate Mend support eight out of ten. We have a shared channel with support on Slack. Their representatives are there to answer our questions or provide clarifications. If we have an issue, we can pose the question, and they respond. We can also create a ticket in their portal. The response time varies based on the severity of the ticket, but it's pretty normal to get a response within an hour. .”

Verified user

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

Read full review

“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 would advise potential users to go through the documentation extensively. The documentation is pretty extensive. It's easy to miss some points in the initial setup itself. If the initial setup's gone wrong, it is difficult to debug it once the infrastructure is up. Therefore, start slow. If the deployment is done correctly, it's only a matter of two files after that for each project that you scan.

I’d rate the solution a nine out of ten..”

Kevin Dsouza
Intramural OfficialIntramural at Northeastern University

Read full review

“I rate Mend an eight out of ten. If you're considering Mend, you should look at your integrations and see what's best suited. It's good having a dashboard, but you need to ensure it supports the tools you use. They tried to sell a SAST product but weren't mature enough for us to take that on board.

If I were to give somebody advice, I would advise against the SAST solution because they're relatively new in the market. Try a demo first. The SAST solution is fast and does what we need it to do. However, you should ensure you're covered integration-wise..”

Kieran Whelan
Principal Security Engineer at Texthelp Ltd.

Read full review

“I rate Mend an eight out of ten. I deduct two points because you may not get coverage for all the package managers. But that's where your team needs to work with the vendor to get that supported. It is a collaborative effort to get more support based on your needs. The company was helpful and responsive, so we were able to influence their roadmap to get some of these capabilities enabled for us.

They have been particularly helpful in getting support for Python package managers. We didn't have the file support and Conda package manager, but they stepped up and provided that capability. You need to have a little patience to evaluate and ensure all the tools meet your requirements. If you need anything, you have to work on getting that support..”

Verified user

Sr. Manager at a financial services firm 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 aat 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 Pitney Bowes Inc.

Read full review

“I would rate the solution a nine out of ten.

As a deployment admin, I would say the solution is straightforward to deploy, and deployment is simply the beginning of the process. Then comes the discipline of running scans along the life cycle of a project and deciding to accept or ignore the yielded alerts. This isn't a daily process, but it's an integral part of every project's workflow, and we have successfully made this an embedded part of our product development. Over time, our users have realized the advantages of using this software and appreciate the deployment.

Our staff must be open to change, especially when adapting to alerts and violations yielded by scans. Every scanned report has its interpretations and challenges, which is where input from the Intellectual Property team and Mend's technical team comes in. They support us throughout the product development process and help us calibrate our interpretations of reports. This gives us a clear picture of whether we are legally and technically conforming to our project and company requirements.

I'm a deployment manager, so I don't know if the merge confidence feature is used, as I'm not involved in projects throughout the entire development cycle. Some teams may be using it, but I can't say with confidence.

We use the SaaS version of the solution, which provides full compliance when it comes to privacy. At no point can Mend view our source code, and we have a complete legal understanding with them.We currently don't use any other products in conjunction with the SCA product because we are at the beginning of our exposure to these tools. We are in the process of evaluating the tools, and we have a relatively elaborate process. It's also essential to consider different tools fairly by comparing like with like and having consistent parameters for comparison. That process can take some time and requires some patience. These kinds of evaluations should not be rushed, and it's okay to take weeks or even months to determine if a new tool can be a commercial and technical success within an organization..”

Verified user
IT Service Manager at a wholesaler/distributor with 51-200 employees

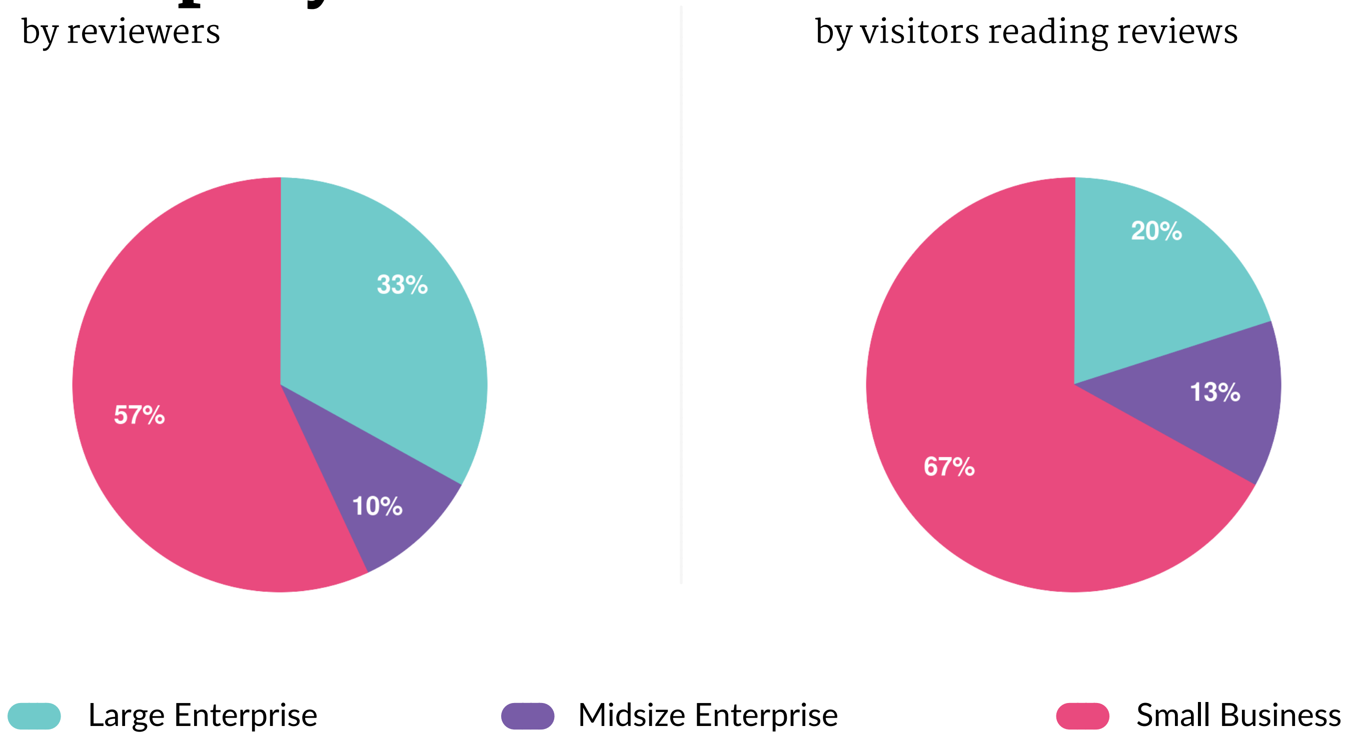
Read full review

Top Industries

by visitors reading reviews

Financial Services Firm	16%
Computer Software Company	15%
Manufacturing Company	11%
Insurance Company	5%

Company Size



by reviewers

by visitors reading reviews

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 software running on AWS and other platforms. 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