



Veracode

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 5

Valuable Features..... 6 - 12

Other Solutions Considered..... 13 - 15

ROI..... 16 - 18

Use Case..... 19 - 21

Setup..... 22 - 25

Customer Service and Support..... 26 - 28

Other Advice..... 29 - 34

Trends..... 35 - 36

About PeerSpot..... 37 - 38

Product Recap



Veracode

Veracode Recap

Veracode is a leading provider of application security solutions, offering tools to identify, mitigate, and prevent vulnerabilities across the software development lifecycle. Its cloud-based platform integrates security into DevOps workflows, helping organizations ensure that their code remains secure and compliant with industry standards.

Veracode supports multiple application security testing types, including static analysis (SAST), dynamic analysis (DAST), software composition analysis (SCA), and manual penetration testing. These tools are designed to help developers detect vulnerabilities early in development while maintaining speed in deployment. Veracode also emphasizes scalability, offering features for enterprises that manage a large number of applications across different teams. Its robust reporting and analytics capabilities allow organizations to continuously monitor their security posture and track progress toward remediation.

What are the key features of Veracode?

- Static Analysis (SAST) - Scans source code for vulnerabilities before deployment.
- Dynamic Analysis (DAST) - Examines applications in a running state to detect flaws in real-time.
- Software Composition Analysis (SCA) - Identifies risks in open-source libraries and third-party components.
- Manual Penetration Testing - Offers expert analysis for more complex vulnerabilities.
- Integrations with DevOps tools - Seamlessly integrates with CI/CD pipelines for automated security checks.

What benefits should users consider in Veracode reviews?

- Early detection of vulnerabilities - Helps developers fix security issues early in the development process.
- Scalability - Supports organizations with large-scale application portfolios.
- Compliance support - Ensures applications meet various security standards and regulations.
- Developer training - Provides tools for educating developers on secure coding practices.
- Comprehensive reporting - Offers detailed reports that track remediation and risk trends.

Veracode is widely adopted in industries like finance, healthcare, and government, where compliance and security are critical. It helps these organizations maintain strict security standards while enabling rapid development through its integration with Agile and DevOps methodologies.

Veracode helps businesses secure their applications efficiently, ensuring they can deliver safe

and compliant software at scale.

Valuable Features

Excerpts from real customer reviews on PeerSpot:



“Veracode Fix has affected our time to remediate security flaws in cases where we've been able to use it correctly because the proposals were on point, and it's been great.”



Verified user

Head of Security Architecture at a healthcare company with 5,001-10,000 employees



“All three of Veracode's offerings are valuable: SCA, SAST, and DAST. It helps identify security loopholes right in the development phase, allowing developers to get feedback around what kind of vulnerabilities exist as soon as they check in the code or even before that in their IDE.”



SrikanthRaghavan

Principal Architect at a consultancy with 11-50 employees



“The best features in Veracode include static analysis and the early detection of vulnerable libraries; it integrates with tools such as Jenkins.”



Himadri Subudhi

Works

- ✓ “Veracode has impacted our overall security posture because we are from a security background. Every week, we review the dashboards of open findings.”



Dristi Kurre

Lead Information Security Analyst at a financial services firm with 10,001+ employees

- ✓ “The good thing about Veracode is that when one scans the respective application code, all the people who are part of the transformation project can update their reviews. If there are any security flaws or vulnerabilities identified, they are able to provide sufficient justification or details about the security flaws.”



Brintha Prabakar

Lead Automation Quality Engineer in Leading UK Bank at a consultancy with 10,001+ employees

- ✓ “The most valuable features include the total developer experience, along with regulator exposure and DevOps pipeline. It encompasses everything as an enterprise solution.”



Verified user

IT App Security Senior Analyst at a transportation company with 10,001+ employees



“It makes it very easy to track and monitor activity.”



Alejandro Mosso

Senior Solutions Architect at IDS Comercial

What users had to say about valuable features:

“We do not have many Veracode features yet. We are going to discuss expanding the subscription next year. Currently, Static Analysis is really good at scanning our code for vulnerabilities. Software Composition Analysis is also required for the upcoming rights from the EU Cyber Resilience Act, which is quite useful, and I am using them both. Both features are really important for us since we're using only Veracode..”

Andrei Kriukov

Application Security Specialist at Herrenknecht

[Read full review](#)

“Veracode has impacted our overall security posture because we are from a security background. Every week, we review the dashboards of open findings. We use both Veracode and Fortify findings, as we are using two separate tools – one for SAST and one for dependency-related issues. When we highlight these in our meetings every day, it gives us a picture of the timeline needed to fix the code. We are using that feature regularly, and it helps significantly..”

Dristi Kurre

Lead Information Security Analyst at a financial services firm with 10,001+ employees

[Read full review](#) 

“My impressions of Veracode's best features indicate that it doesn't have what I need. It's hard to integrate and perform hybrid analysis mapping. The threat modeling components aren't detailed enough. The deciphering of the results is challenging as they're hidden, making it difficult for a non-security user or normal IT developer to understand it.

We have about 100 to 200 licenses, with a very big portfolio of 500 systems, and people still don't understand it. Training 7,000 developers isn't feasible. We had training with Veracode where they conducted a major session, but nobody understood it. These developers can't be expected to remediate and configure the tool properly for comprehensive scanning. Instead, they turn everything off and only scan a very small line of code, which doesn't benefit the agency..”

Verified user

Manager at a government with 10,001+ employees

[Read full review](#) 

“One of the aspects I appreciate most about Veracode is that even though we have a license for developers, we don't get charged by the users who don't develop code but are only trying to access the platform to see the reports or the dashboard, such as architects who do some code reviews but don't develop. That's a nice feature that doesn't happen on other platforms that we analyzed.

Another feature that we appreciate significantly is Veracode Fix and how it's integrated with Visual Studio Code. Even though it has some room for improvement, the key usage for us is to be able to solve everything. The developers also learn how and why they have to solve the security vulnerabilities detected. At the same time, they are developing the feature. Veracode Fix has affected our time to remediate security flaws in cases where we've been able to use it correctly because the proposals were on point, and it's been great..”

Verified user

Head of Security Architecture at a healthcare company with 5,001-10,000 employees


[Read full review](#) 

“The most valuable features include the total developer experience, along with regulator exposure and DevOps pipeline. It encompasses everything as an enterprise solution. In an enterprise, you want developers to be able to do things easily. You want to be able to monitor development in IDEs and the environment states of working pipelines. You want to integrate DevOps pipelines that do scan assessments and evaluation, and promotion to later stages in the pipeline and testing cycles. You still want your security team to be able to access data or pull information for evaluations or regulatory compliance, and report back to corporate compliance.

For the teams that use it, it does affect the time to remediate security flaws. It fixes issues directly in the IDE while you're doing it..”

Verified user

IT App Security Senior Analyst at a transportation company with 10,001+ employees

[Read full review](#) 

“It has met the company's requirements. Nowadays, we are talking about AI code generation. The company is required to leverage the existing code scan to see whether it can support scanning the code that is generated from GenAI before pushing that code to the developers. The developer wouldn't know whether this code is secure or not. Usually, we do the static scan first, but now with a code generator, we want to ensure that it generates secure code.

It did the job. Just before production, we did a scan and ensured that there were no critical or high-criticality issues before going to production. I think that helps to sanitize the code without going into a peer review. We have an automatic scan that catches all these things first, so it's beneficial.

This is especially true for the library because most of these static code scans or software component analyses scan the third-party library that has a CVE or CVSS finding. But if it's a custom-built library that isn't known to the public, it's unclear whether there's a vulnerability or not. Currently, it lacks the ability to trigger on those. We probably have to use a different solution for that..”

Verified user[Read full review](#) 

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

Other Solutions Considered

“When I joined the company, I was given Veracode. The decisions were made before I joined the organization. They had just bought it and needed a specialist for this, and I was the specialist..”

Andrei Kriukov


Application Security Specialist at Herrenknecht

[Read full review](#) 

“I wouldn't be inclined to take a 10-minute callback to discuss my experience with Veracode because I don't prefer it, so I don't think it would be a very good review. I'm looking to replace it..”

Verified user

Manager at a government with 10,001+ employees

[Read full review](#) 

“In my last company, they used Veracode, and then they transitioned to Snyk. The price point was the first priority we looked at. Secondly was the integration—whether it had deeper integration with our system, and was easy for our developers to enroll and use. After a trial of 12 months with Veracode, we decided to move to Snyk..”

Verified user

[Read full review](#) 

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

“Previously, we did a comparison between Veracode, Synopsys (which is Black Duck), and Snyk. We did our own internal review. Veracode needs to shift to a more modern approach because it still feels traditional in its way of doing code scanning compared with others, such as Snyk. They still use a base app, although they have a web version as well, but the integration part could be more seamless. I'm comparing it side-by-side with Snyk, as I'm also a heavy user of Snyk. Those aspects can be improved..”

Verified user

[Read full review](#) 

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

“We did not use a different solution before Veracode. Veracode is our first solution.

I did not work directly with competing solutions similar to Veracode, but I attended several meetings with different companies to explore similar tools. They did not provide anything better than Veracode, and since I had already implemented Veracode in our CI/CD, there was no need to change the solution. I only saw Checkmarx as a competing solution. Though I did not try it myself, from what they showed me, it appeared quite similar but was not better than Veracode..”

Andrei Kriukov

Application Security Specialist at Herrenknecht

[Read full review](#) 

“I do have experience with other testing tools such as Mend and Polaris. The main differences between Mend, Polaris, and Veracode lie in the specific functionalities and how each integrates with enterprises. Overall, the basic functionalities remain similar. In comparing Veracode's breadth of end-to-end testing versus Mend, I find Veracode to clearly be a winner in the SCA segment. Other than that, both are pretty much equal in the SAST and DAST areas..”

SrikanthRaghavan

Principal Architect at a consultancy with 11-50 employees

[Read full review](#) 

ROI

Real user quotes about their ROI:

“The ROI is in terms of time savings and security. If an attack happens because of a vulnerability, it costs a company and impacts its reputation. No one should be compromising on security..”

MukeshSaha

Associate Principal, Software Engineering at LTI - Larsen & Toubro Infotech

[Read full review](#) 

“Since the Cyber Resilience Act is in motion, we need to provide static analysis and dynamic analysis, which we do not have right now. We must do it, and Veracode is a great tool for this purpose. We cannot sell our products without complying with this act, so Veracode is helping us achieve this..”

Andrei Kriukov

Application Security Specialist at Herrenknecht

[Read full review](#) 

“It is too early for that, but Veracode will save us development effort and time. That will be the return on investment for us in the future. We will be able to measure its overall cost-effectiveness by comparing what we are paying for the service and how much developer time it is saving. .”

ShubhamSharma5

Senior Consultant at Material Vision

[Read full review](#) 

“It saves us around 30% of the time. It is worth the investment because security must be the first step when developing an application. You use someone's data, especially if you work with e-commerce, banking, health, or welfare applications. You need to be very aware and secure about it.

Each user's data must be protected, and their privacy should not be compromised. So, it is very important to maintain the security configurations and ensure there are no vulnerabilities. I believe it is worth the investment..”

Sajal Sharma

Test Analyst - Security at Net solutions India Pvt.


[Read full review](#) 

“Especially in banking, security is a must-have. If we have weaknesses in security, it will cost a lot. For example, hacking or people trying to access their networks. The scanners of Veracode bring status of the weaknesses in the current infrastructure.

It scans and provides reports regarding the servers, the network, and the applications running on those servers. It's a very valuable kind of solution. Trying to do it manually would be costly and increase the risk of mistakes if we try to identify all those bugs in the architecture. Using an automated tool brings cost reduction and more security..”

AlejandroMosso

Senior Solutions Architect at IDS Comercial

[Read full review](#) 

“For us, it wasn't the most expensive solution proposed. Part of our decision to get Veracode was that when we evaluated against other products, Veracode was cheaper. What they need to measure is that you need a tool that is efficient and works for your products and how you develop, which has a nice level of detection and a low level of false positives. We make an evaluation and only choose tools that offer a good balance between providing good detections and a low amount of false positives. What was happening with SonarQube was that we had lots of false positives, making teams not care about the vulnerabilities because most were false positives. Regarding price, the evaluation should focus on how efficiently they will recover their investment, considering the time saved through the use of Veracode Fix, for example, and the ability to fix code at dev time compared to the problems faced when fixing after the product is already deployed..”

Verified user

Head of Security Architecture at a healthcare company with 5,001-10,000 employees

[Read full review](#) 

Use Case

“My usual use case for Veracode involves integrating automatic scans for each of our pipelines, which starts every month automatically without my intervention. I review the results, and if there are any changes, such as new issues, flaws, or outdated components, I address this task with our developers..”

Andrei Kriukov

Application Security Specialist at Herrenknecht

[Read full review](#) 

“I have experience with Veracode, as I did download it, and our cyber team manages that. I've used Veracode for quite some time, more from a user perspective, not really as an admin person to run the scans. I share my role with Veracode by normally receiving the results and then analyzing them from there, as I was looking for options..”

Verified user

Manager at a government with 10,001+ employees


[Read full review](#) 

“It helps with intelligent software composition, ISC, allowing us to test fast and get fast feedback around third-party library vulnerabilities, and have a quality gate around the CVEs, and so on.

I work as a digital consultant helping customers with their digital transformation side, with the primary focus on reliability engineering, SecDevOps, and Cloud. I have multiple clients using this same product. My clients are from different industries such as retail, consumer goods, travel, hospitality, and energy..”

SrikanthRaghavan


Principal Architect at a consultancy with 11-50 employees

[Read full review](#) 

“We use the scan and code scanning functionality. Those are the main ones. I just changed my role, so this company is using Veracode, but I've been using it for quite some time before joining this new company. It is currently only managing the source code review. We have other tools that we integrate as such as infrastructure as code, container security, cloud misconfiguration reviews, and others. So it's part of the overall security posture. I can't say that it's solely for our entire security posture because it just manages a subset of one of the security requirements, which is the source code review..”

Verified user

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

[Read full review](#) 

“My use case for Veracode includes utilizing the SSA and SAST modules as part of improving the code that we are developing in the company, and we have 130 developers that we are trying to onboard in this platform. We have been able to onboard 100 more or less in these months, and the idea is to change the way they are developing because we want them to heavily use the IDE integration.

We mostly use Visual Studio Code, and we have them using the integration plugin with Veracode so that they can fix the security issues at dev time. When we have the product in the pipeline, and we run the scans again, it's a green light..”

Verified user[Read full review](#) 

Head of Security Architecture at a healthcare company with 5,001-10,000 employees

“We have used Veracode only for third-party libraries until now. We have automated that and have onboarded the Dev team to directly scan from their pipeline. We have integrated the CI/CD in that way. We try to see whether the third-party libraries they have been using are safe versions, and if not, we are able to guide them along. For static scan, we primarily use Fortify. With Veracode, I do not have much experience because Fortify is our main tool.

We are the security personnel. We give proper guidance to the development team and use Veracode whenever scans are in queue or stuck, helping to provide clarity on findings. We have guided the development team with the tool so that, as security auditors, we do not have to do that. We have given guidance to the development team since every release needs code without vulnerable dependencies or vulnerable code. We have guided them in a way that they can access such tools, where they can see the report, and where vulnerable code is present..”

Dristi Kurre[Read full review](#) 

Lead Information Security Analyst at a financial services firm 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.

“When it comes to the initial setup, it's both straightforward and complex. While the product is mature, it requires integrators. For example, I'm using GitHub Flow, but the GitHub app to plug in is not sufficiently mature..”

SrikanthRaghavan

Principal Architect at a consultancy with 11-50 employees

[Read full review](#) 

“Without the documentation, the deployment and initial setup is complex. I tell my developers who are interested in Veracode that with this documentation, everything is possible because it is really thorough and helpful. At first, it was somewhat complicated, but with the documentation and time, it became a really good experience. After that, it became very easy and quick..”

Andrei Kriukov

Application Security Specialist at Herrenknecht

[Read full review](#) 


“The initial deployment was difficult. We had some problems with the SSO integration. But Veracode found a fix, and they are delivering the final solution to production. It took us a lot of time to get that mitigation, and it's not that fast to onboard the dev teams. We are having meetings with each team depending on the language they are using and the type of application; it may be really fast or take up to a week for them to have the product integrated. My expectation was that it was going to be faster..”

Verified user[Read full review](#) 

Head of Security Architecture at a healthcare company with 5,001-10,000 employees

“It is somewhat complex compared to Fortify. As a Fortify user for almost five years, I find Veracode complex, but others in my team who have used it for eight to nine years don't find such issues. When we were doing manual scans before CI/CD integration, it was easier.

It took approximately four to five months to onboard the solution because it was new to developers as well. There was a certain process to be followed to get access and integrate it into the CI/CD tools. We had to explain the report format to them, showing where they could find vulnerabilities and how they could fix the code, including finding safer versions of libraries and dependencies. This took almost half of 2023, and now in 2025, they do not need our help except for technical problems when there are numerous scans in the pipeline..”

Dristi Kurre[Read full review](#) 

Lead Information Security Analyst at a financial services firm with 10,001+ employees

“The deployment is complex. There are multiple things we need to check before getting our application to deploy.

So, the setup's complexity could be improved or simplified, in my opinion.

The scan doesn't take that much time to complete. You just need to sync it with your application and the scan. You just need to make the configuration and use the API into AWS or Jenkins pipeline. So, it will take five to six hours to integrate, not more than that. But with the tests, to make sure that it is working fine with the deployment and all, it takes one day.

The solution doesn't require any maintenance; at least I didn't face anything. I just wait for the upgrade. It gets upgraded with the latest known vulnerabilities, and it gets better and improved. .”

Sajal Sharma

[Read full review](#) 

Test Analyst - Security at Net solutions India Pvt.

“The initial deployment was pretty straightforward. It's on-prem so there was no deployment strategy to follow. It took one to two days to deploy and check everything. A team of three to four people worked on the deployment. It depends on the project's complexity as well. As a DevOps engineer, I support a lot of projects within our organization, and the deployment varies from project to project.

In my department, we handle six to eight projects and each one needs a Veracode scan before deployment. As a company, we have multiple locations and departments but only the DevOps team of eight people has access.

The way we work with Veracode is that we have integrated it with Jenkins. We upload the artifacts to the server, trigger the Jenkins job, and the Veracode scan is generated. We have set everything from the Jenkins pipeline. The scan is automated using Jenkins, which means there is no need for maintenance. If there are new steps implemented in the pipeline, there might be some overhead, but it doesn't need any maintenance. We just set the port and everything works fine..”

Akash R.

[Read full review](#) 

DevOps Engineer at a consultancy with 10,001+ employees

Customer Service and Support

“The technical support by Veracode is good because we have encountered problems before, and the team supported us effectively. For technical support, it deserves a rating of eight out of ten..”

Dristi Kurre

Lead Information Security Analyst at a financial services firm with 10,001+ employees

[Read full review](#) 

“I have communicated with the technical support of Veracode a couple of times, and this was a really great experience because these professionals know their material. They understood us immediately and helped us with our problems within half an hour. It was incredible. I would rate them a ten out of ten..”

Andrei Kriukov

Application Security Specialist at Herrenknecht

[Read full review](#) 

“I didn't get involved much with asking them questions. During the initial phase when we started integrating, they were very helpful, but after they deployed the license and everything, we haven't reached out to them to ask any other questions. It's gone into autopilot. Once you have the license, everything just continues as it is..”

Verified user

[Read full review](#) 

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

“I would rate Veracode's customer service or technical support as not great, probably a four out of ten. Anytime we use the advisory to speak with an advisor, they are either too technical or have no understanding. We have a weekly meeting with Veracode because we have our own business relationship manager. He attends the calls without a technical person or lead architect to facilitate questions. When 40 people are on a call asking questions about turning off the API or fixing issues, the response is often that they cannot answer. The service is either a hit or miss, which is why I rank it low..”

Verified user

[Read full review](#) 


Manager at a government with 10,001+ employees

“We have an enterprise license and direct connection with the Veracode team. I consulted their team about a couple of issues or bugs in the product that weren't matching our requirements, and we provided feedback that they took back to address.

I would assess their help as eight out of ten in terms of how they assist with the issues I bring to them. It's good to have access to their team at no extra cost with the license, as most SaaS platforms include consulting as part of their offerings, but access to the engineering team is crucial for faster feedback on the product fix process..”

SrikanthRaghavan

Principal Architect at a consultancy with 11-50 employees

[Read full review](#) 

“I have contacted the technical support and customer support. With Veracode's technical support, for some issues, it has been really difficult for them to understand the problem, and they ask us to do some tests we've already told them we completed in the first ticket. I think there is room for improvement there. However, we are also working with premier support, where we have an engineer assigned to our account. When we work with him on one of our problems, it gets solved much faster. Now we always try to add this engineer to all of our tickets so that we can solve everything faster. That's because we have the premier support as part of our agreement..”

Verified user

Head of Security Architecture at a healthcare company with 5,001-10,000 employees

[Read full review](#) 

Other Advice

“I haven't used the Veracode Fix feature that produces AI-generated fixes.

The fact that Veracode doesn't scan source code, only binary code, is not a concern because we have certain projects that work with this approach. The AI functionality could be innovative, though I haven't experienced it yet. Regarding the breadth of Veracode's end-to-end testing versus competing solutions, I would rate it as eight out of ten.

Overall, I would rate Veracode a seven out of ten..”

Dristi Kurre

Lead Information Security Analyst at a financial services firm with 10,001+ employees

[Read full review](#) 

“My impressions of Veracode's policy reporting for compliance with industry standards and regulations are hit or miss. While it has industry standards built in, our organization has different policies that are more structured. Each policy must be set up individually, requiring comprehensive legwork.

For example, if there's a policy for a deprecated protocol in an internal-only system, Veracode still reports it as an issue. This creates unnecessary work for internal systems that aren't public-facing and have lower risk. Configuring the tool to align with policies for sensitive, public-facing systems based on law and NIST requirements requires reviewing each line individually, which becomes a two-year project.

My impressions of Veracode's ability to prevent vulnerable code from going into production is that the static code analyzer portion is adequate.

On a scale of 1-10, this solution rates a 5..”

Verified user

Manager at a government with 10,001+ employees

[Read full review](#) 

“I would rate Veracode's ability to prevent vulnerable code from going into production at an eight out of ten because AI is evolving, and there are other tools emerging that help by proactively changing the code without needing the developer to take action, ensuring that pull requests are handled before going into production.

We just got the Veracode Fix feature, but we need to understand it more deeply to know if it just performs code fixes or handles dependencies as well. Can it arrange or adjust my versions to make sure that the library that I'm using does not have any vulnerabilities? We have not enabled AI-generated fixes because we need to try it out and see how it performs, especially concerning human intervention in auto-upgrading or automatic patching in production. I am yet to explore the continuous delivery and continuous deployment aspects to provide feedback on that.

I would recommend Veracode to others, as it maintains strong industry adoption.

Overall, I would rate Veracode an eight out of ten..”

SrikanthRaghavan

Principal Architect at a consultancy with 11-50 employees

[Read full review](#) 

“We don't use some of these tools because we don't have the license for them. We are not using Veracode for DAST or for manual penetration testing, but we are using the other ones, and they give visibility through the process. I think that Veracode does it, but since we are not using DAST, we are only part of the development process before going to the runtime environments. So we are not checking anything on runtime. That part of the process, where you have the product running and you make real tests on the running product, we are not solving with Veracode, but that's mainly because we don't have the DAST licenses. The way we are using Veracode now means that since we haven't finished the

rollout yet, we are not putting any restrictions on our pipelines so that they can only go to production if Veracode didn't find any critical vulnerability. Now, we are not using it as a blocker, so it depends on the team. Some teams don't want to appear in red in the reports from the last pipeline scan, so they are delivering much more secure code to production. Other teams don't care and still deliver with the same vulnerabilities, but that's something that varies from team to team. Generally, most teams have improved a lot, for example, by updating all the libraries and reducing all the critical and high vulnerabilities, delivering to production only with low or medium vulnerabilities..”

Verified user

Head of Security Architecture at a healthcare company with 5,001-10,000 employees

[Read full review](#) 

“I am working with the latest version of the features. Since starting with Veracode, I would rate the benefits as six or seven out of ten. It could be better if we had more high severity issues, but fortunately, we do not. It is a good sign that developers who are not in cybersecurity understand its value.

Regarding the solution's policy reporting for ensuring compliance with industry standards and regulations, I am using standard policies. I rated it five out of ten because we have not used it properly yet.

Veracode provides visibility into application status at development phases. We tried [IDE](#) scans for the developer stage of products, but it was not fully compatible with our [IDE](#). It works in CI/CD as mentioned.

We do not currently have the Veracode Fix feature that produces AI-generated fixes. The fact that Veracode does not scan source code, only binary code, does not concern us as we have other tools for that purpose.

I would rate Veracode an eight out of ten..”

Andrei Kriukov

Application Security Specialist at Herrenknecht

[Read full review](#) 

“The integrated [IDE](#) tool enables users to get instant feedback in real-time on the code itself, rather than waiting for it to go through the CI/CD pipeline and get the result. They can instantly review their code on demand, which is quite beneficial.

For my previous company, when they first adopted source code review, they went for the open-source option first. I always advocate for people to go with the open-source option to understand what the features are and how exactly the source code scanning looks. Once comfortable with it, or if certain features are needed, then look for the enterprise version. Sometimes for different companies, especially

small businesses, they couldn't afford Veracode because of the steep price.

Regarding integration, apps such as [Jira](#) and [Confluence](#) are important. The main thing was that it's fully and deeply integrated with the user and the repository, like [Confluence](#). [Every](#) time there's a report, we can immediately generate a ticket from Snyk to [Jira](#). It helps the developer get notified about issues after the scan. Then they fix the issue, tag the ticket as resolved, and once it's marked as resolved, we will do the rescan.

As a beginner, the interface is quite straightforward. People will not get confused. The technical report is professional and can be used by regulators. I can simply export it as a PDF and then share it with a regulator or any auditor for their review.

Regarding mobile code support, such as iOS, Kotlin, and others, the results were not really promising. For Java and C#, it's very good. They are pioneers in that. But for mobile development, if you're a mobile company that builds mobile apps and you have iOS, Objective-C, Swift, and Kotlin, that area needs to be polished.

I rate Veracode a seven out of ten..”

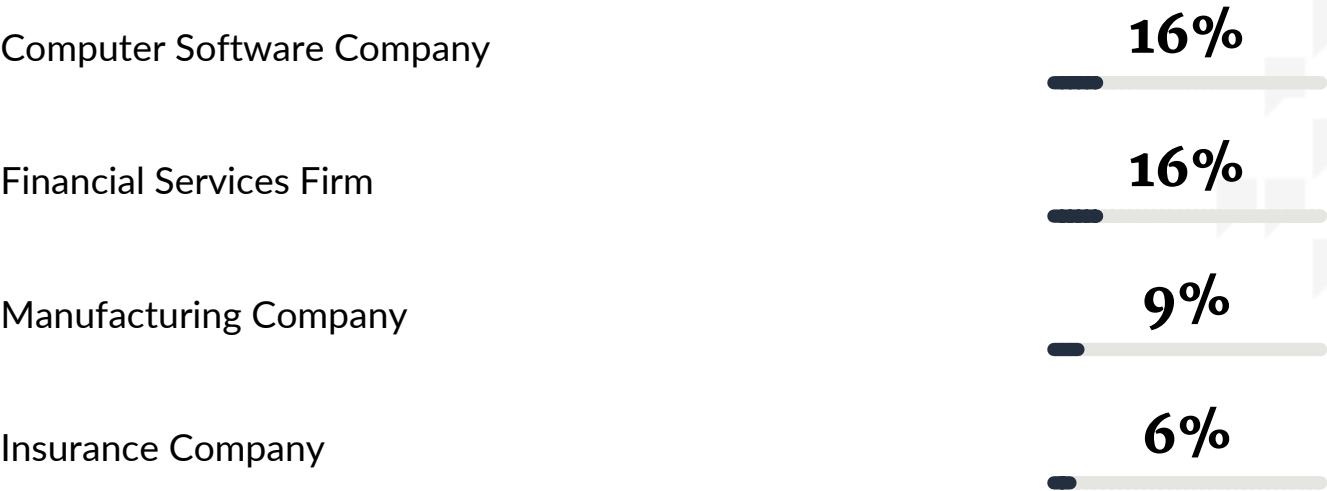
Verified user

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

[Read full review](#) 

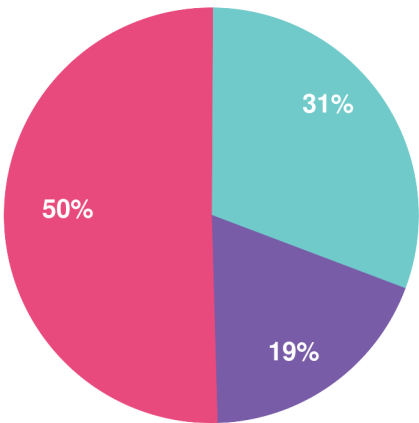
Top Industries

by visitors reading reviews

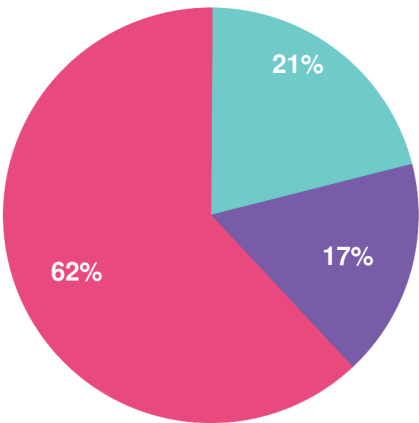


Company Size

by reviewers



by visitors reading reviews



Large Enterprise Midsized Enterprise Small Business

About this buyer's guide

Thanks for downloading this PeerSpot report.

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

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

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

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

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

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

[Get your personalized report here](#)

About PeerSpot

PeerSpot is the leading review site for 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