PeerSpot

Case Study

Veracode

Shiva Prasad Reddy

Program Analyst at a tech services company with 10,001+ employees

Review by a Real User

Verified by PeerSpot

What is our primary use case?

In my previous company, we had a healthcare app. We used Veracode to run a spontaneous static analysis as well as dynamic analysis, to resolve our vulnerabilities. We were releasing versions every month. Each month we were looking at the results of Veracode and fixing the problems.

How has it helped my organization?

It helps fix a lot of flaws and bugs. As a developer, you look at things with a different perspective with the Veracode results. You can see that certain things can be implemented in another way, how they can be more secure. As a result, it helps improve your level of understanding and decrease the number of production issues.

Using Veracode, it was very interesting to see the difference when I compared things over a three-month timeline. During the initial three months, when I started using Veracode, I found the percentage rate of flaws was around 60 to 70 percent in the entire file we were uploading. After using Veracode over the next three months, our score decreased to a 30 to 40 percent flaw rate. We were able to do our quarterly development in a very secure way.

For example, we recently encountered a flaw that might be exploited. We implemented a function to store passwords that were encrypted. That functionality was written in a pretty vulnerable manner. By looking at the code, we could see, "Okay, this might be exploited." But when Veracode pointed out multiple times, "This might be vulnerable," and

"This might be vulnerable," it helped us improve our developer standards. It gave us a brief idea of how this particular code implementation could be improved.

There is also a feature called Veracode Pipeline Scan which provides instantaneous feedback. That was a major addition to our process and has worked out very well. Developers get instant feedback about their flaws, making them easy to fix while in pre-production. That is one of the major boosts that we have implemented. It enables our developers to fix things in parallel, and that has saved time, about 20 to 25 percent, and resulted in better coding. As a security guy, I can see the differences between the initial processes and the processes we have six to eight months after implementing Veracode Pipeline Scan and Veracode in general.

Overall, it has reduced the time that we used to spend working manually to pinpoint the issues that we found. Veracode makes it an automated process. Also, we can use it in parallel. If Veracode is the main "hub," we can have "sub-hubs" such as static analysis and Veracode Pipeline Scans. Both can be done simultaneously, reducing the manpower required by a lot, and providing correct results. And it has improved our understanding of the different kinds of flaws and vulnerabilities that are in the report. Veracode, as a tool, has made things better.

In terms of security posture, when I had just joined my previous organization, there was a meeting about client feedback. Initially, their comments were that things were not very stable. They said it was easy to steal data. After using Veracode, and as our developers adapted the tool and developed secure code, the client's feedback was that things were pretty stable and good. At first, the feedback was very ruthless. We were not up to security standards. But once we started using Veracode, it became the main pillar of our security. We overcame certain challenges and the client feedback was pretty good.

What is most valuable?

It yields around 90 percent accurate results. It pinpoints the errors. Its accuracy is very interesting. It also elaborates on flaws, meaning it provides you with details about what is valid or not and how something can be fixed.

Another valuable feature is in the dynamic analysis, which provides information on which libraries are outdated so that we can improve them and get them up to date. We found a lot of outdated libraries in use in our organization. As a result, it has improved our stability. The software composition analysis keeps you updated on each kind of data it reports on, including libraries and third-party DLLs.

What needs improvement?

There is a sandbox limit of 10 so any company using Veracode needs to plan for only

having those 10 sandboxes. If they increased that to 25 or 30, the scan time would decrease and the results should be more effective.

There is also a size limit of 100 MB so we cannot upload files that are larger than that. That could be improved.

Also, the duration of the scan is a bit too long.

For how long have I used the solution?

I used Veracode in my previous company but recently changed to a new company. Overall, I have used it for around 1.5 years.

What do I think about the stability of the solution?

Its stability is fine. On a scale of one to 10, I would give it a seven for stability.

What do I think about the scalability of the solution?

It's a scalable solution.

We have it implemented in two offices, the main office in the US and a single office in India. There are only 10 to 12 people using it in our organization, meaning in India. I am not aware of how many users there are in the US.

How are customer service and support?

Their support team needs to respond in less time. It takes a lot of time for them to respond. When we reach out, we are waiting, most of the time, for two or three weeks to get a reply from them. That is the one major piece of feedback I have for Veracode.

Their technical support is very good, except for the response time. When we are stuck with something technical, they explain how to use it in multiple ways. They are supportive and that is pretty good.

How would you rate customer service and support?

Neutral

Which solution did I use previously and why did I switch?

We were using a couple of other tools along with Veracode. One was SonarQube and the other was Acunetix.

What other advice do I have?

The false positive rate is pretty low. When I started using Veracode, there were a lot of false positives, but that number became notably smaller. There are some false positives because

new types of flaws are generated for each new version.

Initially, in general, whenever you see any kind of false positives or true negatives, it reduces your confidence. But whenever the reports are generated by Veracode, as developers we can understand that they show certain patterns of what might be a false positive. So we get an idea that this kind of a flaw might be a false positive while this kind might not be a false positive. We get clarity about the reports sent by Veracode. At a certain point, we might be sure that we can explain all the false positive data to management so that they can look into them and understand: If this kind of data or this kind of code flaw comes up, it is a false positive. We can easily associate these scenarios with false positives because they are normal and common.

During the initial phase, false positives affect our time because we can't deduce any conclusions. Static analysis is the kind of process in which you will encounter false positives in certain cases. But after a couple of implementations of machine learning, the results should be pretty accurate and the false positives should decrease.

Preventive maintenance is critical. Per my experience with Veracode, there are certain maintenance issues, but they are the normal types of things.

I would highly recommend Veracode, but initially, don't do a deep dive into the tool. Take a couple of licenses to start adapting to the tool and work out how it works and whether it's suitable for your development processes and developers, and get their feedback. I highly recommend it because it's a real time-saver, provides stability, and improves your organization's productivity.

Which deployment model are you using for this solution?

On-premises

Read 23 reviews of Veracode

See All Reviews