

Case Study

Veracode



Daniel Krivda

DevOps Engineer at a insurance company with 10,001+ employees

- ✓ Review by a Real User
- ✓ Verified by PeerSpot

What is our primary use case?

We use it for static scans. It is mandatory in our company for every sort of project.

Veracode provides the organization an understanding of security bugs and security holes in our software, finding out if the software is production-ready. It is used as gate management, so we can have a fast understanding if the software is suitable for deployment and production.

My job is to help projects by getting the data integrated in Veracode. I don't own the code or develop code. In this area, I am a little bit like an integration specialist.

We use Azure and AWS, though AWS is relatively fresh as we are now just starting to define guidelines and how the architecture will look. Eventually, within a half year to a year, we

would like to have deployments there. I am not sure if dynamic scanning is possible in AWS Cloud. If so, that would be just great.

How has it helped my organization?

The possibility to integrate Azure is very valuable because you can have every build integrated into the content integration pipeline. So, you can have every build scanned and determine when a new bug was introduced. Thus, you can keep great track of your code's security.

What is most valuable?

You can easily integrate it with Azure DevOps. This is an added value because we work with



Azure DevOps. Veracode is natively supported and we don't have to work with APIs.

What needs improvement?

Third-party library scanning would be very useful to have. When I was researching this a year ago, there was not a third-party library scan available. This would be a nice feature to have because we are now running through some assessments and finding out which tool can do it since this information needs to be captured. Since Veracode is a security solution, this should be related.

I would recommend that they keep working on the integrations. For Azure DevOps, the integration is great. I am not sure what the integration possibilities are for the Google platform or AWS, but I would suggest every other platform should have this easy and great integration. It takes a lot of time for companies, so this feature is a big plus.

For how long have I used the solution?

I have been using it for about three years.

What do I think about the stability of the solution?

There have been no issues at all. There has been no downtime registered.

How are customer service and support?

I worked with the technical support to integrate some things. One of our private cloud providers only had old routers. It was possible only to open network connections to IP addresses, while Veracode only provided the URL in their guide. So, I asked the technical support if it was possible to provide some fixed URLs that we could give our provider since it is unfortunately against the concept of the cloud to provide the IP addresses that work just for some time. The technical support's response was within a day, and it was prompt and clear. Also, all their reasoning made sense so the support was very good. I would rate the technical support as 10 out of 10.

How would you rate customer service and support?

Positive

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

We also use SonarCloud, which is a code quality tool. We use both of them because both these platforms are good in some areas. While the Veracode is very good at finding security-related issues, the SonarQube Sonar suite is very good at determining code quality. Also, when I was looking into the topic, the SonarQube team



answered that there is no point for them to go further into code security since there are already great competitors who have years of experience and development behind them, specifically mentioning Veracode as masters in their field. That is the reason why we use both solutions: We benefit from using them both. These solutions compliment each other.

Which other solutions did I evaluate?

I evaluated WhiteSource Bolt specifically for third-party library scanning, but I did not have a lot of time to create a proper PoC. I had a call with WhiteSource and told them that I would like to do a PoC, but I was not very satisfied with their support. It was like, "Just try the free solution then contact us again." However, the free solution didn't provide me enough things to make a decision. So, I just put it off until sometime possibly in the future. If Veracode offered third-party scanning, then we wouldn't need WhiteSource Bolt at all.

What other advice do I have?

If you have Azure DevOps and would like to understand your code and how secure it is, then there are not a lot of better options. Also, there are not many choices in this area at the moment. Once your code is scanned by the static scan of Veracode, you get some evaluation scores based on some criteria. For the management,

when it is above a certain number, it is fine, but when it is built below, then it is no-go for production. Even though there is a possibility to create a sandbox environment for projects, they don't get it. That is understandable to me. I try to explain to them that there are no issues if you are working in a development environment and you get difficult scans. It is fine then because you can create a sandbox environment, which will not screw up or make the production releases worse because it is in a separate bucket.

We are happy using the solution. I would rate it as nine out of 10.

Which deployment model are you using for this solution?

Public Cloud

If public cloud, private cloud, or hybrid cloud, which cloud provider do you use?

Microsoft Azure



Read 23 reviews of Veracode

[See All Reviews](#)