PeerSpot

Case Study

Veracode

Zach Handzlik

Release Manager/Scrum Master at Amtech Software

Review by a Real User

Verified by PeerSpot

What is our primary use case?

We use it primarily for our application security concerns. We use the dynamic, static, and SCA scanning tools. We run our static scans after the code is compiled, and that gets uploaded automatically through our DevOps tool. We have installed an agent in one of our cloud servers that is behind a firewall to run the dynamic scan against the runtime. We run our SCA scans when we do the static scans, which is after compilation.

How has it helped my organization?

Prior to using Veracode, we hadn't really looked into security features or thought about security in the same way that we have since we started using Veracode. We were focused on what you hear about in the news, such as making sure that it is HTTPS secured. We hadn't really dug into the nitty gritty of application security and scanning our source code, running it against a runtime environment, and looking at the actual third-party solutions that we integrate or use in our code. Veracode has helped with our mindset as an organization to start thinking about things more securely by design rather than as a reactive measure. We're being more proactive with security.

What is most valuable?

Veracode's integration with our continuous integration solution is what I've found to be the most valuable feature. It is easy to connect the two and to run scans in an automated way without needing as much manual intervention.

We feel very confident about Veracode's ability to prevent vulnerable code from going into production. Having the stamp of approval helps not only from a marketability standpoint but also from an overall good feeling within the organization that we're doing our part to help keep our code free from vulnerabilities.

This solution provides visibility into application status at every phase of development. It goes from compiling the code all the way to running it in production. It covers all major aspects of the SDLC. We run static scans and SCA scans early on in the process to make sure that we catch any code that is insecure by design. If we are able to catch it earlier on, before it's actually out in the production environment, it reduces costs. The dynamic scans are run further along in our QA process. That is, once we've deployed the code and have it in a runtime environment, we run weekly scans in a dynamic environment against the code runtime to make sure that there aren't any new vulnerabilities that got introduced. We are looking at doing manual penetration testing in 2023, where we would be using a spinoff of the code that was released to the customers to make sure that there aren't any holes through which a nefarious actor could get in and exploit what was built.

Veracode's false-positive rate is low. The few instances when it looked like there were false positives, the issues were found to be either true vulnerabilities or things that were that way by design. If a developer thought that there would be a ton of false positives when using the tool, it would then diminish the value of actually using the tool. Veracode touts itself as being a tool with the lowest false-positive rate in the market. It gives inherent confidence in the tool itself, and developers are more inclined to think that if it found something, it's pretty likely that it is not a false positive. They would then work to prove it wrong rather than discounting it without even looking into it.

We haven't really found many false positives with static analysis, and there hasn't been a significant impact on our time and cost related to tuning, leveraging data, and machine learning.

Continuous integration linking definitely saves a lot of time because it takes away the step where a developer needs to manually upload the code every time to do a scan. It can run in the background, and having the Visual Studio plugin includes it directly in the development environment. If developers do get assigned a bug that they need to fix, they can pull it right up in their development environment and not have to log in to the portal. It will all be right there.

I'm primarily the one who has been involved in DevSecOps, and Veracode has definitely reduced my time. If we had gone with a conglomeration of open-source tools, it would've taken me a ton more time. Whereas with Veracode, all the documentation is out there, and I'm able to integrate everything that I need from a usability standpoint. I don't have to learn a new tool every time I need to integrate a new security scanning option. It has helped me

tremendously and has saved me a lot of time.

What needs improvement?

I do expect large applications with millions of lines of code to take a while, but it would be nice if there was a possibility to be able to have a baseline initial scan. I know that Veracode touts that there are Pipeline Scans that are supposed to take 90 seconds or less, and we've tried to do that ourselves with our ERP application. However, it actually times out after two hours of scanning.

If the static scan itself or another option to run a lower tier scan can be integrated earlier on into our SDLC, it would be great. Right now, it takes so long that we usually leave it till a bit later in the cycle, whereas if it ran faster, we could push it to the time when a developer will be checking in code. That would make us feel a lot more confident that we'd be able to catch things almost instantaneously.

For how long have I used the solution?

I've been using Veracode for a little over a year now.

What do I think about the stability of the solution?

I haven't had any stability issues, bugs, or glitches.

What do I think about the scalability of the solution?

The scalability is really good. I recently added to the solution some new applications that I learned about late in the game. There were probably 10 that I had to add in rapid succession and scan as well. It was very quick and painless.

How are customer service and support?

Veracode's technical support is very responsive, and I've heard back within 24 hours regarding a couple of issues I've entered. We have actual consulting calls, which are a scheduled event, and I like the way they handle those as well. I have nothing but good things to say about them and give them a rating of ten out of ten.

How would you rate customer service and support?

Positive

How was the initial setup?

I was involved with the initial setup of Veracode, and it was straightforward. We had a third-party vendor who was evaluating it, so a little bit of the setup was done. However, adding a new

application to the tool is easy and self-explanatory. It doesn't take much time at all, and the documentation is out there if we need to look up anything.

What about the implementation team?

We implemented it with the help of a third-party vendor. They had two people on their team who were working on the deployment along with me. My responsibilities included adding all of our software to the tool to run scans against it, integrating it with our DevOps solution, discussing the tool itself with internal stakeholders as to how they can use it and showing programmers how to use the tool from an internal adoption standpoint.

What's my experience with pricing, setup cost, and licensing?

I know that Veracode is a semi-pricey solution. If you are serious about security, I would recommend that you use an open-source option to learn how the scanning process works and then look into Veracode if you want to really step up your game and have an all-in-one solution.

Which other solutions did I evaluate?

We evaluated a couple of open-source tools such as Snyk and SonarQube against Veracode with the help of a third-party vendor. We didn't use any of those and landed on Veracode because of the Veracode Verified seal. This, along with Veracode being the market leader, gave Veracode an edge over the others.

The main difference between Veracode and the solutions we evaluated is that Veracode is an all-in-one solution. Though an open-source solution would've been more cost-effective, we would've had to use a bunch of different tools. It would have required more knowledge to do the integration piece and would've taken a lot more time and effort. There would have been invisible costs associated with it just by the virtue of time. In comparison, Veracode's dynamic scan, static scan, and software composition analysis are all in one place.

What other advice do I have?

My advice would be to look at the open source tools out there and see how far along you are in your security journey and what your needs are. If you're looking for the best in the market, Veracode is a great option, as far as paid solutions go, because it's a one-stop shop. If you have more time at your disposal and you don't mind integrating some solutions, then I'd recommend an open-source tool. However, if

you have the resources, I would definitely recommend going for Veracode.

On a scale from one to ten, I would rate Veracode at nine.

Read 23 reviews of Veracode

See All Reviews