O1

Veracode

Review From A Customer

From IT Central Station, the leading review site for enterprise technology solutions.

Review by a Real User

Verified by IT Central Station

Chief Technology Officer

Dave Cheli

WHAT IS OUR PRIMARY USE CASE?

The primary use is as a static analysis tool. But we also use Greenlight and dynamic, and we're currently having a manual penetration test.

HOW HAS IT HELPED MY ORGANIZATION?

Firstly, it prevents me from putting out software that has security vulnerabilities, which is a big thing and can be one of the most important things. Also, we just finished a vendor due diligence with a very large company that wants to do business with us, and one of their security questions was "Do you do static analysis?" I was able to just send a very professionally done report. They know Veracode and they said, "Okay, great. This is terrific."   That very reason is why, three years ago when I first got to this company, I said, "We have to get hooked up with Veracode right away, so it's not like an afterthought." Because I'd been in a situation where you do it after the fact and you end up with 3,000 errors, medium to critical errors. It helps us put out better software more quickly, and gives me the piece of mind that we've done everything we can to prevent any security exploits. It's something that our customers don't think about, and the benefit would be that as long as there are no data breaches, there's no hacking within our system, they get a non-functional benefit. We work with pharmacies and they just expect that the system is secure. I would view that as a benefit to them - maybe something that they don't think about - but nonetheless, it's there.

WHAT IS MOST VALUABLE?

Certainly it eases integration into our workflow. Veracode is part of our Jenkins build, so whenever we build our software, Jenkins will automatically submit the code bundle over to Veracode, which automatically kicks off the static analysis. It sends an email when it's done, and we look at the report. Once it's set up - and it's pretty easy to set up - it pretty much just works and I don't really have to think about it, outside of whenever I get my emails to look at the reports. It was a very easy integration that we did within the first week of going live with the software. So ease of use, ease of integration.

Veracode

WHAT NEEDS IMPROVEMENT?

The Web portal, at times, is not necessarily intuitive. I can get around when I want to but there are times when I have to email my account manager on: "Hey, where do I find this report?" Or "How do I do this?" They always respond with, "Here's how you do it." But that points to a somewhat non-intuitive portal. With that said, I hate when companies redo their portals all the time. So it's kind of a catch-22, but that would be my only critique.

FOR HOW LONG HAVE I USED THE SOLUTION?

Three to five years.

WHAT DO I THINK ABOUT THE STABILITY OF THE SOLUTION?

It's always been pretty rock solid.

WHAT DO I THINK ABOUT THE SCALABILITY OF THE SOLUTION?

No scalability issues that I'm aware of.

HOW IS CUSTOMER SERVICE AND TECHNICAL SUPPORT?

Exceptional.

WHICH SOLUTIONS DID WE USE PREVIOUSLY?

Veracode was really my first introduction to static code analysis. The way I came across it in my previous company was, they were going through security due diligence and we didn't have any code analysis software. The company, a very large health plan, said, "Here are three that we recommend." Veracode happened to have been one of them, along with HPE and another company, maybe it was IBM, I don't know. We took a look at all of them and we made a decision to go with Veracode.

HOW WAS THE INITIAL SETUP?

It was easy. It's very straightforward. There's nothing complicated about it.

WHAT WAS OUR ROI?

I haven't really thought about cost savings related to code fixes, since we implemented Veracode, other than: It's always easier and much cheaper to catch errors and fix them before you go to production, versus catching them while in production. Just like it's much easier to fix things before production, as opposed to having somebody hack your system and to find out that you have a cross-site script error. But again, I've never quantified it in terms of whether it's saved me money. Just off the cuff, the cost of the license is small in comparison to the value it brings. I don't have to buy the software myself, I don't have to have specially trained security professionals that monitor this stuff. But I haven't really broken it down to quantify it into dollars, as such.

Veracode

WHAT'S MY EXPERIENCE WITH PRICING, SETUP COST, AND LICENSING?

I think it's a great value. It's at a price point that a small company like mine can afford to use versus, if it was too exorbitant, I wouldn't be able to use this product. About licensing, just go ahead and get them. Get a license at the beginning of a project. Don't wait until the end, because you want to use the product throughout the entire software development lifecycle, not just at the end. You could be surprised, and not in a positive way, with all the vulnerabilities there are in your code.

WHICH OTHER SOLUTIONS DID I EVALUATE?

When I was at the last company, I looked at HPE (now Micro Focus) Fortify vs Veracode and maybe IBM had a product, but they were overly complex and overly expensive. I remember talking to our Veracode account rep, who also was my account rep originally here at Focus Script, and she did a fabulous job of explaining it, doing a demo, showing how easy it was to use, and that's what sold me. Again, it was recommended from a very large health plan as one of the more reputable systems out there.

WHAT OTHER ADVICE DO I HAVE?

CA Veracode provides application security (AppSec) best practices and guidance to our teams in a couple ways. First of all, they have an e-learning module that has courses that we have required our developers to take. That's a best practice. Secondly, when we do have errors, Veracode is always available, their consultants, to help us either mitigate the error, or provide technical assistance on pointing exactly where the problem is and how we could probably fix it. I'm always amazed at how knowledgeable they are. They also have what's called a Software Composition Analysis that can point out errors and fixes for third-party software frameworks, which is very nice. The list goes on... And again, having received, early on, education from them on how best to integrate this in the workflow, those are areas where we've relied on best practices from Veracode. I'm in healthcare, and it's very important - and I'm sure in other industries just as well - but the stakes are very high. If we get hacked, if there's a data breach, it could put us out of business. It's a very good price point for a small company to have these kinds of capabilities, something we can afford for our application. I am very likely to recommend it to colleagues. As I mentioned, I brought it to this company, and I've already recommended and provided references to a few other companies over the last couple of years.