VERACODE

Software Composition Analysis

Gaining visibility into your open source code reduces the risk of breaches from vulnerabilities. High-performing companies rely on Veracode's flexible SaaS platform to provide the insights they need to easily identify open source libraries in use, their vulnerabilities, licenses, and risks to their applications – protecting both their applications and their customers' data through better DevSecOps practices. The following are the technology aspects of our solution that set us apart from the competition.

NVD vs Our Proprietary Database

The National Vulnerability Database, although very robust, is not able to keep up with the sheer volume of vulnerabilities being disclosed and/or updated daily. In addition, the only way that a vulnerability makes it into the database is if a software developer or an independent security researcher submits it to the NVD. It is not uncommon for vulnerabilities to be fixed, but never disclosed or submitted to the NVD.

Veracode's approach

To combat this, we have developed our own database that includes all of the open source vulnerabilities in the NVD, as well as our own list of vulnerabilities in open source libraries that have not yet been disclosed to the NVD. In many cases, the vulnerabilities we find and record have either not been disclosed yet and are in the time between patching and full public disclosure, or in some cases, there was never any intent to disclose the vulnerability and its fix. There is a third category we track, which are "Reserved CVEs." We take the Reserved CVE IDs from the NVD and then find the vulnerabilities in the public repos, in order to give you a head start on the fix prior to full public disclosure.

Machine Learning

In open source projects, bugs are typically tracked with issue trackers, and code changes are merged in the form of commits to source control repositories. Thus, if an organization is able to monitor all of these repositories and review each new bug issue and commit message, they could identify potential vulnerabilities. However, there are tens of thousands of open source repositories, with hundreds of thousands of bug-tracking issues and commit messages to comb through, with new ones hitting every day.

Veracode's approach

Our system uses natural language processing and real machine learning to identify potential vulnerabilities in open source libraries with a high level of accuracy. By analyzing the patterns found in past commit messages and bug-tracking issues using machine learning, our model can identify when new commits or bug issues resemble a silent fix of a potential vulnerability. These potential vulnerabilities are then raised to our security research team. These silent fixes can be a silent killer for your data protection.

License Database

In addition to tracking security vulnerabilities, which is the main focus of our technology, we also offer the ability to identify the most common sets of open source licenses that can pose both business and financial risk to organizations. We are able to help companies identify open source licenses like Apache, MIT, MPL, BSD, CCDL, and GPL to name a small few. We are working to identify and add more license types that our customers are looking to identify in their code.

Container Scanning

With Veracode SCA you can scan your Docker image or container directly in your CI system or from your CLI. We return open source libraries that the base OS image uses, as well as any globally installed packages. For a strong AppSec process, customers must scan the application and the container separately, in order to get a full picture of the potential vulnerabilities introduced to their final application. We support CentOS/RHEL as the base image, and packages installed globally using YUM.

Call Graph

You can run the scanner interactively from a command line or automatically as part of a continuous integration process. By integrating with your build process, you always know exactly what code is being used.

With each scan, it generates a call graph of your application and generates a complete and accurate dependency graph that describes with absolute precision what versions of open source libraries are being used. Using both the dependency graph and call graph, the scanner then performs control flow analysis to determine, with the best level of precision possible, if your application is actually using open source code in a vulnerable way.

Scanning Agent

The agent is deployed with a single line added to your CI system, or within your CLI, by performing a CURL command, and pulling the most up-to-date agent from Veracode. On subsequent scans, the command checks if there is a newer version of the agent and pulls that version down to your environment.

The agent is most effective when scanning your system during the time of an application build, since it is able to create a call graph of the application to understand how it is composed, and how data and controls flow through your application. This allows us to get better coverage of your code, and identify vulnerable methods in supported languages.

SaaS Based Solutions

When it comes to scaling your AppSec needs, the easiest way to do that is with a SaaS based vendor. Our cloud based AppSec solution ensures that you always have access to scan your applications, and the results, no matter where you are. Your organization does not have to worry about costly on-premises equipment, redundancies, nor backups.

Security Research Team

The security research team is responsible for taking all of the data that our machine learning system sends us, and reviewing each potential vulnerability to ensure that it is in fact real. If there are any false positives that return, the team adds this feedback into the system to better tune the algorithm over time.

1st & 3rd Party Code Coverage

The greatest strength of Veracode is the ability to cover your entire Software Development Lifecycle (SDLC) from end to end. From scanning the very first few lines of code added by a developer with Greenlight, to scanning a fleet of applications deployed in production with Dynamic Analysis, Veracode provides you the coverage you need. So while it's critical to ensure you are aware of the vulnerabilities in any open source libraries being used, it's equally important to scan your 1st party code for any critical security flaws.

Complete Bill Of Materials

Veracode provides security and development teams with a complete bill of materials of every library being used by your application, and allows you to review this list in aggregate at the portfolio level or by each individual application.

Dependency Graphs

A lot of the work our engine does centers around mapping out your application and all of the open source libraries that the application depends on: both directly pulled in by developers, and indirectly pulled in from those direct libraries. Other SCA solutions on the market struggle with this dependency mapping, often reporting many duplicates of the same vulnerability for a single application. This redundancy in reporting can lead to extreme bloat of results reporting, generate many false positives, and give your development teams the difficult task of identifying what's real versus what's not.

It is important to realize that, again, just because your development teams are only using 10 open source libraries, they could actually be pulling in hundreds of different libraries indirectly. Our scanner identifies all of these, the versions being used, and any vulnerabilities that they contain. And for supported languages, it identifies the call stacks and traces the vulnerabilities through your application to identify those that actually impact your application and leave it open to exploits.

Vulnerable Methods

Most SCA solutions simply look at your application's dependency file to determine what versions of which open source libraries are being pulled into the application. They then compare that list to a vulnerability database, usually the NVD, and pull back a list of libraries that have reported vulnerabilities in them. However, just because a vulnerability exists in one part of the code, doesn't necessarily make the entire library vulnerable.

Veracode's approach

We solve this problem with our agent, and the way we discover open source dependencies in an application. The call graph creation that happens by the agent (discussed in the previous section) allows us to see how data and controls flow through your application – which includes determining if that data is flowing through the vulnerable part of the open source library being used. If it is, we indicate back to the developer that this is in fact a vulnerable method, and it is causing your application to be vulnerable to exploits. When we scan with vulnerable methods, we find that up to 90 percent of the vulnerabilities reported are not likely to actually impact the code. While we definitely recommend developers stay on top of the latest up-to-date version of every library they use, in reality development and security teams have to work together to make trade-offs between security and speed. With vulnerable methods, developers can tackle the vulnerabilities that are actually likely to make their application vulnerable first, reducing their risk by the most in the shortest amount of time. Today, vulnerable methods is available for Java, Ruby, Python, and .NET.

Your AppSec Program With Veracode

There are a number of different places where you could start your application security program, and a lot of different paths to mature your program – but there are not a lot of companies that can help cover your needs from end to end. When assessing your options for your AppSec partners, you need to look for a company that can cover the entire software development lifecycle (SDLC), with a strong focus not only on first- and third-party code, but also the ability to actually implement a mature program. Veracode is the market leader in application security, and our years of experience have shown that those companies that evaluate their first-party code, plus open source libraries, and do so early, midway, and late in the SDLC have the best coverage. With Veracode, you can ensure a scalable, cost-effective AppSec program that helps make security part of your competitive advantage.

Learn more about Veracode Software Composition Analysis

VERACODE

You change the world, we'll secure it.