VERACODE

Veracode Vendor Application Security Testing

DID YOU KNOW?

- ✔ On average, Veracode finds 83 vulnerabilities per third-party application.
- ✔ A Veracode Fortune 100 Customer found that over 90% of the third-party software they tested had significant compromising flaws.
- ✔ Information and communications technology supply chain risk assessment should be integrated to the overall enterprise risk assessment processes throughout the organization.

NIST Special Publication, 800-161

"Piggybacking on third-party suppliers is now a well-worn page in attackers' playbooks.."

Dark Reading

Assess security of the software you buy

Manage security assessments across your vendor landscape

Commercial applications have an average of 83 vulnerabilities, but procurement teams are doing little to assess the risks at time of purchase, increasing their organizations' security and audit risks. In addition, regulations, such as PCI DSS, NIST SP 800-161, FS-ISAC and MAS, require assessing software supply chain risk. Vendor self-assessment questionnaires do little more than check boxes, and penetration testing is time-consuming and expensive. Assessing third-party software is even more challenging when vendors have to provide access to their source code, which many regard as confidential intellectual property.

Veracode Vendor Application Security Testing (VAST) provides a scalable program for managing third-party software risk. Build your program based on a decade's worth of best practices to ensure success and see a simple pass or fail for each vendor application. Because Veracode scans binaries rather than source code, vendors will be more comfortable with the assessments because they don't have to disclose their intellectual property. With Veracode, you can scale your program without adding specialized headcount and manage the entire program on a single platform.

Build your program based on a decade's worth of best practices

Veracode has helped thousands of organizations with their application security program over the past 10 years. We work with you to formulate a strategy for contacting your independent software vendors (ISVs), define policies for compliance that can include a mix of automated and manual testing methods, and get them into compliance. Once you have reached out to your software vendors based on our proven process, we'll handle the rest of the program management, including follow-ups with vendors, assessments and removing any roadblocks to compliance. If you already have a vendor assessment program, we can help you to improve and scale it.

See which vendors comply with your corporate policy

No matter how complex your corporate policy is, you'll be able to see a simple pass or fail for each vendor application, including static and dynamic scans, software composition analysis and manual penetration tests. Reports include a bill of materials comprising all open source and commercial components that enable you to quickly assess where your organization is exposed as high-profile open source vulnerabilities are discovered. Policies can cover several regulations requiring an assessment of software supply chain risk, including PCI DSS, NIST SP 800-161, FS-ISAC and MAS.

VERACODE

Reduce vendor resistance by scanning application binaries

Software vendors will be reluctant to share the source code of their applications because they consider it their confidential intellectual property. Veracode's patented technology scans binary code, so ISVs don't have to share source code with a third party. Because Veracode conducts the application scans in its cloud-based platform, software vendors cannot game the system by "tweaking" scanning parameters to comply with policy.

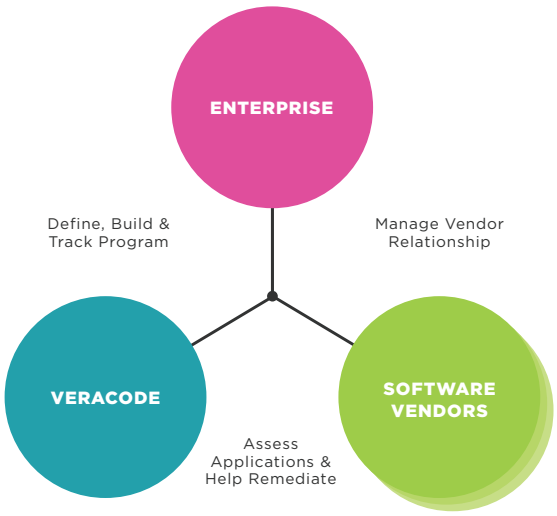
Scale your program without adding specialized headcount

Finding security professionals is hard, but finding talent with a background in application security and program management is even tougher. With Veracode, you get instant access to a broad range of services that serve as an extension to your team. Our security program managers will work with you to onboard software vendors to facilitate assessments, and our application security consultants are available to developers who need coaching on how to address vulnerabilities. Veracode can even review software vendors' mitigation proposals to provide you a qualified third-party opinion that will stand up to auditing scrutiny.

Manage your entire program on a single platform

Your entire program is managed through the Veracode Application Security Platform, which provides you an overview of all of your vendors' compliance statuses. The platform helps foster collaboration between Veracode, the software vendors and you to track progress and results. In addition to seeing a simple pass/fail, you'll be able to access detailed reports on each application. Analyze your application landscape and get a global view of vulnerabilities across all applications on the platform.

Contact Veracode to learn how we can help assess your vendor supplied applications.



The Veracode Application Security Platform

The Veracode Application Security Platform offers a holistic, scalable way to manage security risk across your entire application portfolio. We offer a wide range of security testing and threat mitigation techniques, all hosted on a central platform, so you don't need to juggle multiple vendors or deploy tools. Application security cannot be solved with technology alone, so our security program managers will work with you to define policies and success criteria and create a strategic, repeatable way to tackle your application security risk. Veracode educates developers with actionable results, one-on-one coaching, and a variety of training, so they can effectively fix existing flaws and code securely moving forward.

www.veracode.com