Manage the risk of open source components in your applications

Open source components are a blessing and a curse. They help accelerate your application development at no cost but put your organization at risk of getting breached and failing compliance audits. Here are your odds: 44% of applications contain critical vulnerabilities in open source components. Applications have an average of 46 components, and knowing which ones you are using is necessary to defend yourself when major vulnerabilities like Heartbleed and Shellshock are announced. This is why several compliance regulations require inventories of open source components so that you can address risks.

Veracode Software Composition Analysis (SCA) helps you build an inventory of your open source components to identify vulnerabilities, covering open source and commercial code. The Veracode Application Security Platform analyzes both proprietary and open source code in a single scan, providing you visibility across your entire application landscape. When a big vulnerability hits the news, Veracode helps you quickly identify which applications in your organization are vulnerable. Because no technology is a silver bullet, Veracode supports your program’s people, processes and technology by coaching your engineers on secure coding practices, managing your remediation and mitigation process, and discovering known and unknown vulnerabilities through its highly scalable SaaS platform.

Assess proprietary and open source code in a single scan

Focusing only on proprietary and open source code means you’re blind in one eye — you need to get visibility of your risks across both parts to cover your bases. The Veracode Application Security Platform analyzes your open source components to find vulnerabilities with the same scan you’ve already set up for static binary scanning — without having to rescan the applications. As a result, you’ll reduce integration points, get broader visibility across your application landscape, and assess your entire application against one policy — summarized in a single report.

Manage your remediation and mitigation workflow

The Veracode Platform helps you manage the workflow for remediation and mitigations. Once you find a vulnerability in an open source component, you can immediately see whether the latest version of the component addresses it. Your developers can also access educational resources to help them addressing the security issue.
Get one-on-one remediation coaching for software developers

When vulnerability descriptions and on-demand educational resources are not enough, developers can schedule calls with a Veracode expert to talk through the options of remediating or mitigating the vulnerability.

Identify open source components and new vulnerabilities in your portfolio

Open source vulnerabilities are so impactful because the components libraries are widely used and repackaged in software. When a big vulnerability hits the news, Veracode helps you quickly identify which applications in your organization are vulnerable. This saves precious time as you’re formulating your action plan. You can also manually blacklist certain components, leading to an automatic policy audit fail for any application that uses it.

Identify and remediate vulnerabilities to help comply with industry regulations

Several industry regulations and security frameworks require that you find and patch known vulnerabilities in your applications, including PCI DSS Requirement 6.2, OWASP Top 10 A-9, FS-ISAC, NIST-800-53 SA-12, NIST-800-161 CM-8, and HITRUST CSF v7. Identifying and remediating or mitigating vulnerabilities helps you comply with these regulations and pass audits.

Use a scalable SaaS solution that integrates with your SDLC

Security works best when it’s part of how people do their jobs. The Veracode Application Security Platform integrates with every part of your software development life cycle. The SaaS-based platform reduces your operational overhead and is highly scalable to meet your demands at peak times.

If you’re already scanning your own code with Veracode, contact us to try out Veracode SCA and get visibility into your open source risk — without rescanning your 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