VERACODE

Integrations

Integrate application security into your SDLC

DID YOU KNOW?

- ✔ A major United States insurance company implemented Veracode Developer Sandbox for Veracode Static Analysis to bring application security earlier in the development cycle. Testing reached over 100 applications scanned and over 1,000 developers enabled in the first four months of the program.
- ✔ A global bank integrated Veracode Static Analysis and SCA into its software development lifecycle via build server and IDE integration, enabling it to go from assessing applications only twice a year with a legacy on-premises SAST tool to assessing within each development sprint.
- ✔ A US-based independent software vendor integrated Veracode Static Analysis into its IDEs and build servers, enabling it to scan more frequently and find issues earlier in the development lifecycle. It found over 4,000 issues in the first six months of the program and has fixed 28 percent of them to date.

Develop secure software faster. Integrate Veracode with your business.

Developers and security teams are both challenged to meet security goals in complex environments. Developers already need to manage many separate tools; new AppSec tools that do not integrate well or lack flexible APIs and customizable integrations are met with low adoption, high distraction and a steep learning curve. Likewise, security teams often seek to protect against AppSec vulnerabilities with a web application firewall and are challenged to integrate risk data and program metrics across disconnected AppSec tools without manual effort. As more organizations move to DevOps and reap the automation and speed benefits, AppSec solutions need to keep up or risk being left behind.

Veracode enables organizations to speed applications to market without sacrificing security. The Veracode Application Security Platform integrates with the development, security and risk-tracking tools you already use. And, our flexible API allows you to create your own custom integrations or use community integrations, built by the open source community and other technology partners. Veracode's focus on making security developer-friendly is one reason why we help you go faster, without sacrificing security.

Do security testing early from within your IDE.

Developers work best when tools don't get in their way, which is why Veracode integrates with Eclipse, IBM RAD and other Eclipse-based IDEs, IntelliJ, and Azure DevOps. Before checking in your code, you can start a scan, review security findings and triage the results, all from within your IDE. In addition, you can easily see which findings violate your security policy and view the data path and call stack information to understand how your code may be vulnerable to attack.

Enforce automated security testing from your build pipeline.

Make sure you catch security issues before they get further downstream by integrating Veracode into your Jenkins, Azure DevOps or Team Foundation Server build or release pipelines. You can test in the pipeline or in parallel and can even stop the pipeline if security issues that violate your policy are found. Not ready for CI yet? You can use us in your Maven build too.

Automatically create tickets for security findings. And automatically close them.

Security findings are best addressed by fixing the source of the problem, in the code. But the prevailing approaches—spending all day creating bug tickets by hand, or doing a one-time import into a defect tracker only to have to update the bugs by hand afterwards—are a pain and don't scale. Veracode's defect tracking integrations with JIRA, Azure DevOps, TFS and HPE Application Lifecycle Management not only create defect tickets, but they also automatically update or close them when the code is retested.

VERACODE

Integrate with web application firewalls to block attacks.

Need more time to fix an issue? You can use Veracode DynamicDS findings to automatically generate rules for your Imperva or Apache ModSecurity web application firewall, so you can target just the areas you know have problems.

Incorporate Veracode findings into your overall risk dashboard.

Struggling to tie your application security program to your overall IT and security program objectives? Veracode provides native integration for RSA Archer to make it easier to understand which of your applications may be in violation of your corporate security policies and how quickly the organization is addressing issues. And partner-developed integrations are available for many other GRC and risk management platforms, including RSAM, RiskVision, Lockpath, Symantec CCM, Allgress, Brinqa, Threadfix, Kenna Security and MetricStream.

Integrate with Veracode's APIs.

Need to start Veracode scans or consume Veracode scan results from a different system? Just want to script the process to make it easier? Veracode provides web-native APIs that allow for full automation of the scanning lifecycle, consumption of results and even provisioning and maintenance of Veracode platform user accounts. And you can use a pre-built wrapper library for Java or .NET to include our APIs in your project. Veracode's API customers have already integrated us into many additional SDLC, DevOps and GRC tools including Bamboo, Bugzilla, TeamCity, Ansible and Hygieia.

Integrate with an industry-leading solution that's built for DevOps.

Unlike manual code reviews or penetration tests, Veracode Static Analysis and Veracode Software Composition Analysis are automated processes delivering fast, repeatable, low-noise results. When scanning entire applications in DevOps-friendly languages, more than 70 percent of scans complete in under an hour, and scans of microservices return more quickly. You can check for vulnerabilities in your open source components in the same scan, without requiring additional integration effort into your continuous integration pipeline. It's all backed by the Veracode Application Security Platform, which has assessed over 2 trillion lines of code in 15 languages and 50 frameworks.

Integrations List

Integrated Development Environments (IDEs)	Eclipse*; IBM RAD (9.5 and later); IntelliJ; Visual Studio **The Veracode Eclipse plug-in can often be used with other IDEs derived from Eclipse, but these are not specifically tested.*
Build Servers	Jenkins; Azure DevOps; Team Foundation Server; Bamboo; Ant; Maven
Defect Tracking Systems	JIRA; Azure DevOps; Team Foundation Server; Bugzilla; HPE ALM; Rally* **Community authored integration, available from Github.*
Web Application Firewalls	Imperva; Apache ModSecurity
Governance, Risk and Compliance Solutions	RSA Archer; RSAM*; RiskVision*; LockPath*; Symantec CCM* **Partner maintained integrations, available from the partner.*
Application Vulnerability Correlation Solutions	Kenna Security*; ThreadFix*; Brinqa*; MetricStream* ** Partner maintained integrations, available from the partner.*
Other Solutions	Veracode customers and partners have developed integrations to a variety of other solutions, including the following: Hygieia; Ansible

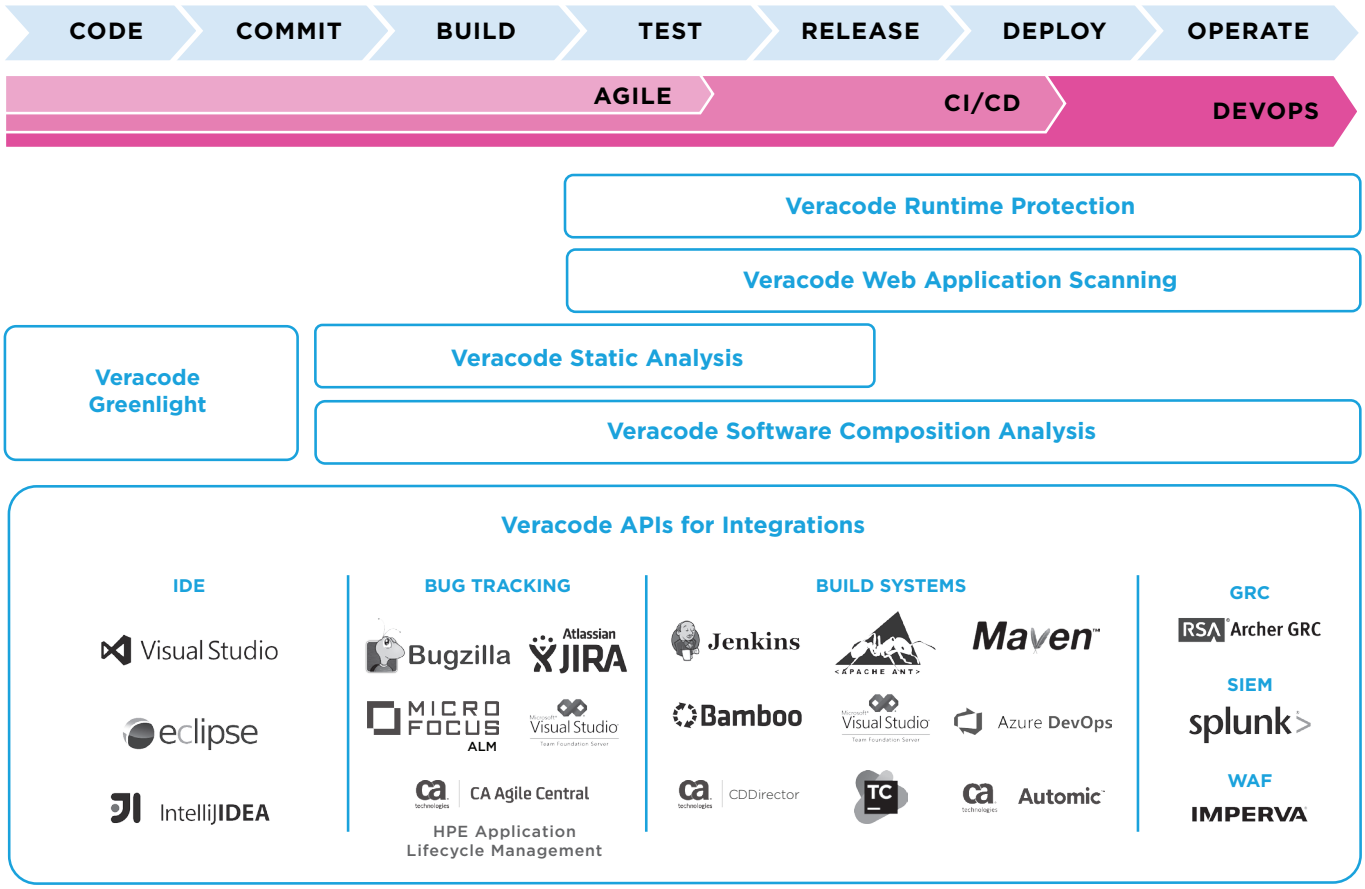

Figure 1 *Veracode integrates with developer and security tools across the entire life of your application.*

The Veracode Application Security Platform

Developers work best with application security tools that disappear into their own tools and processes, such as IDEs, build servers and defect tracking systems. Security teams want to buy developers more time with WAFs, but struggle to write accurate rules; they also need to use security findings to measure risk in central GRC and risk management systems. Veracode integrates with the development and risk tools you're already using so you can easily secure all your applications.