VERACODE STATIC ANALYSIS: THE RIGHT SCAN, AT THE RIGHT TIME, IN THE RIGHT PLACE

BY VERACODE

VERACODE

CHALLENGES WITH STATIC ANALYSIS

Software development is integral for an organization looking to keep up with market trends, remain competitive, and disrupt markets. While the world is innovating through software, all software introduces risk. Most applications are not built with security in mind, making them a top target for security breaches. Despite years of access to security testing tools, 83 percent of applications have at least one security flaw on their initial scan, and two out of three applications fail to pass tests based on the OWASP Top 10 and SANS 25.

Tools are noisy and difficult to deploy

The application security tools of yesterday burden the fast-moving development teams of today with false positives that slow them down. Worse, the noise of false positives muddles developers' view of real vulnerabilities and erodes their confidence in test results. Organizations are taxed with the challenges of scaling on-premises solutions across globally disparate development teams, further slowing teams down, leaving organizations with an approach that runs counter to the needs of their teams and the demands of the business.

Testing doesn't align with modern development practices

Software is being released faster than ever, as 43 percent of development organizations deploy code continuously, and 41 percent deploy between once a day and once a month. Yet 50 percent of development organizations agree security vulnerabilities are discovered most often by the security team after the code is merged in a test environment. Forty-nine percent encounter most delays in the testing phase of the software lifecycle.

Developers not empowered to remediate flaws

Security education is woefully missing from computer program degree requirements, and the majority of developers say that the training they've received in application security is inadequate. When examining the top 40 computer science programs in the United States, Forrester found that zero of the 40 schools require a class about secure coding or secure application design. While security teams try to augment this gap, they are challenged with lack of bandwidth and staffing challenges. The cybersecurity talent shortage is staggeringly high – (ISC)2 estimates that there are just under 3 million open cybersecurity positions globally. This means organizations are not adequately staffed to manage increased risk throughout the security or development organization.

VERACODE

VERACODE STATIC ANALYSIS CAN HELP

Veracode has developed a Static Application Security Testing (SAST) solution that works for organizations seeking to better secure their applications without reducing development velocity within the business.

Veracode Static Analysis harnesses the power of our patented technology to deliver three methods of testing to meet the unique needs of development and security professionals across the Software Development Lifecycle (SDLC). These testing methods are the IDE Scan, the Pipeline Scan, and the Policy Scan, which are detailed more comprehensively below.

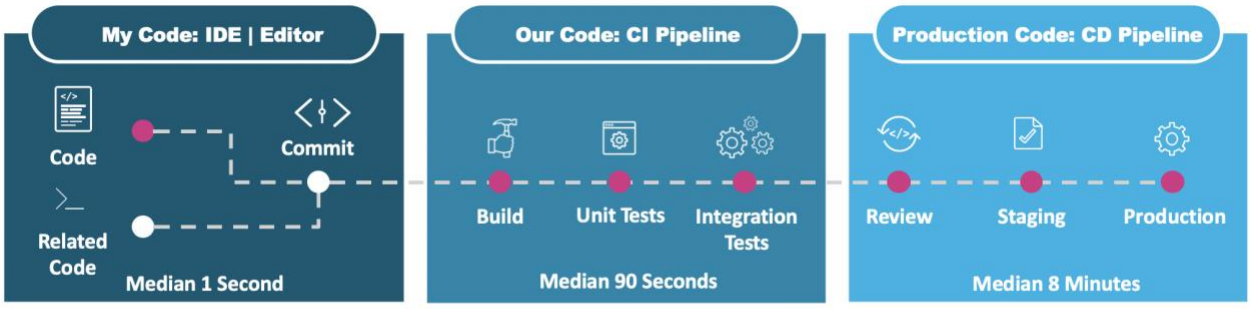
Veracode's centrally managed reporting and analytics helps demonstrate AppSec progress and program success, enabling security professionals to demonstrate compliance to internal stakeholders and compliance auditors. It equips teams with the insight into remediation skills that have been built over time, encouraging developers to share those skills across development teams, further helping to ship secure code quickly. Security professionals can benchmark their performance against other companies in a similar industry to understand the context around their performance and can track the metrics that indicate success.

More than a tool

Veracode goes beyond providing scanning tools to partner with organizations to successfully start and scale AppSec programs. Veracode Customer Success draws on best practices developed through the experience of running more than 2,800 programs, and with over 40 million flaws fixed using our comprehensive SaaS model. Veracode application security experts offer strategic guidance to build, mature, and scale impactful AppSec programs across the entire application portfolio. Veracode's experts extend organizations' teams to provide support with SDLC integration, remediation coaching for developers fixing security defects, and demonstrating program success to key stakeholders using proven metrics. Veracode offers security program management, application security consulting, technical support, and developer training to ensure that your program achieves the desired outcomes.

Seamlessly fit Veracode into your development processes

To confidently ship secure software, you need the right scan, at the right time, in the right place. Veracode Static Analysis provides scans that are optimized for when they are leveraged in the Software Development Lifecycle, and whether the intent of the scan is for full application security assurance, rapid feedback in the pipeline, or individual developer continuous flaw feedback and education.



IDE Scan
Learn as you code and prevent new flaws from being introduced

Pipeline Scan
Provide fast feedback on first-party code

Policy Scans
Centrally managed testing & reporting for security & auditors

VERACODE

Get security feedback as you code

In the pre-commit stage of development, the IDE Scan offers fast and focused real-time static analysis scans for developers as they code. It scans the code that a developer is currently working on and provides real-time feedback to help developers answer the question, "is the code I'm writing secure?" before they commit it into the main repository. In addition to finding flaws, it also helps to accelerate remediation and educate developers through positive reinforcement, remediation guidance, code examples, and links to Veracode AppSec Tutorials. Companies using the IDE Scan have reduced flaws introduced in new code by 60%.

Receive fast results in the pipeline

The Pipeline Scan is purpose-built for DevOps engineers, integrating into the CI pipeline to offer test results each time code is committed. In the build stage of development, pipeline scans with a median scan time of 90 seconds offer fast feedback within a development pipeline in the context of an application in order to answer, "is the code my team is writing secure?" This scan directly embeds into teams' CI tooling and provides fast feedback on flaws being introduced on new commits. Teams can break the build if policy-violating flaws, based on severity or CWE category, are introduced on a commit or net-new security issues are found. Because this scan is performed in line with existing CI tooling, there is no learning curve for development teams.

Background Knowledge

Why embedding testing across the SDLC is so important

Fifty percent of development organizations agree security vulnerabilities are most commonly discovered by the security team after code is merged in a test environment, and 49 percent encounter most delays in the testing phase of lifecycle. When an organization has implemented a CI system, the general consensus is that everything moving to production passes through that CI system. Thus, if you put your security checks into your CI system, then you know that everything moving to production passes through the security scan. Many tools try to embed into the SDLC leveraging only a policy-level scan, but usually miss the mark in terms of speed and as a result, trade off on accuracy and coverage. The result is that solutions either tune out results, creating false negatives, or applications are only scanned late in the testing phase. Veracode optimizes scanning for continuous feedback on every commit, which gives us the most accurate assessment of your code's security and empowers your developers to fix security risk.

Satisfy auditors and achieve compliance

The Policy Scan ensures that applications are meeting policy compliance and industry standards, and creating visibility for cross-functional remediation. The entire application is evaluated against one policy, and its security posture is summarized in a single report from a centralized testing and reporting structure that can be shown to internal stakeholders and external compliance auditors. In the pre-production and production stage, sandbox and policy scans – with a median scan time of 8 minutes - enable teams to centrally manage testing, compliance, and reporting for development management, security teams, and auditors to answer "are my organization's applications secure?" Leveraging the Sandbox Scan, teams can review policy compliance without setting off alerts before promoting the scan to a Policy scan, which provides security reporting and audit attestation. The entire application is evaluated against one policy, and its security posture is summarized in a single report. Integration points are reduced and simplified, giving security teams broad visibility across their application landscape, as well as the continuous feedback needed to improve their overall security posture.

Benefit from Veracode's patented engine

All scan types benefit from Veracode's patented technology, which analyzes dozens of major frameworks and languages with a 1.1 percent false-positive rate. In addition, our SaaS-based approach and integrations make it seamless to deploy and scale application security testing within the development process. Once flaws are identified, teams can leverage in-line remediation advice and one-to-one coaching to reduce mean resolution time. The combination of scanning types tailored to

distinct use cases teaches developers to use the industry's security best practices, and how to prevent flaws from entering their pipeline without impacting velocity. Performing these checks throughout the development cycle allows full application static analysis scans, conducted later in the SDLC, to act as an audit rather than the first means of security testing, which lowers the overall mean time to remediation and cost associated with building secure software.

Get a fast start and scale quickly

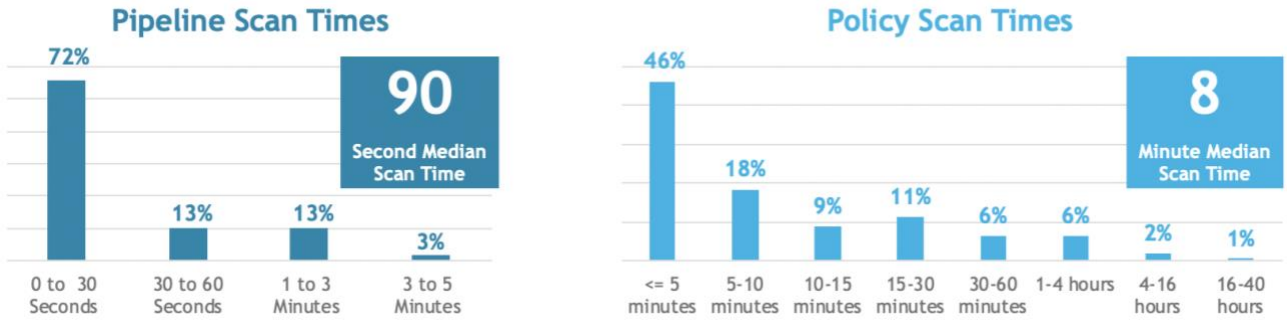
When it comes to scaling your AppSec needs, the easiest way to do that is with a SaaS based vendor. Our cloud based AppSec solution ensures that you always have access to scan your applications, and the results, no matter where you are. Your organization does not have to worry about costly on premise equipment, redundancies, or backups. The proof is in the numbers; Veracode scales to millions of scans a year, all while maintaining rapid scan times at scale with no queuing or configuration required.

2800+
Static Customers

6.3M+
Static Scans in 2019

60.9M+
Unique Flaws Found

Scan time performance:



Focus on fixing, not just finding, with Veracode's remediation guidance

Veracode provides in-depth technical details about every flaw found, including how it was identified, the severity of possible exploitation the finding represents if left unfixed, as well as in-depth remediation/mitigation suggestions.

Understand the severity of your flaws

The Veracode scoring system, Security Quality Score, is built on the foundation of two industry standards, the Common Weakness Enumeration (CWE) and Common Vulnerability Scoring System (CVSS). CWE provides the dictionary of security flaws and CVSS provides the foundation for computing severity, based on the potential Confidentiality, Integrity and Availability impact of a flaw if exploited.

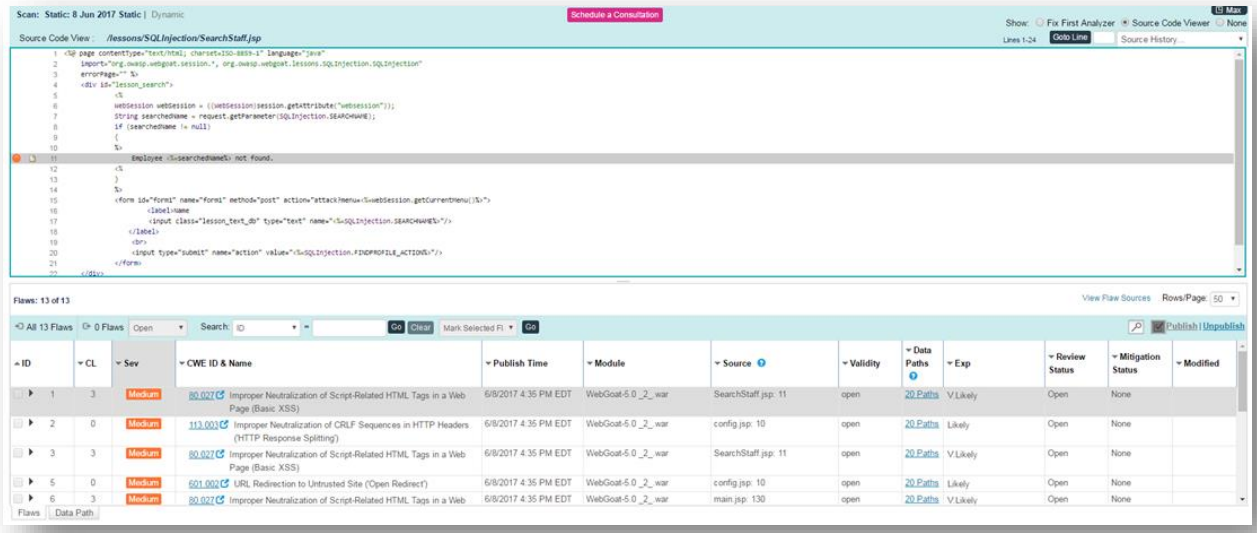
VERACODE

Get in-context remediation guidance

When reviewing a specific finding, Veracode provides written guidance and code samples on how to fix a vulnerability for the specific programming language. If this doesn't help, developers have access to on-demand video tutorials specific to the flaw type and programming language.

Prioritize issues and fix efficiently

When alerted to security issues, developers can triage flaws in the Veracode portal in several ways, including filter findings in the Triage Flaw Viewer. The Fix First Analyzer helps prioritize the issues identified that are high impact and easy to fix. Flaw Sources helps to identify code changes that would eliminate several vulnerabilities at once.



Receive one-on-one advice from a secure coding expert

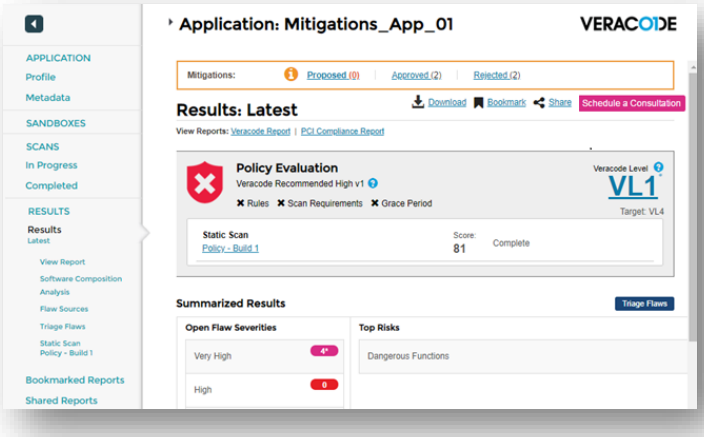
The greatest value our customers get out of using Veracode is not just finding their flaws and vulnerabilities, but actually remediating them. We have set up our solution portfolio to be developer-friendly so that engineers can get the information they need as fast as possible, and begin working on the right path to remediate those issues. However, when developers hit a roadblock, our developer consultation calls come in: developers can schedule calls with our experts who can provide interactive discussions of scan results, and guidance on how to fix the problems we find. Nobody else has the knowledge and staff on hand to help developers produce secure applications every time.

VERACODE

Always have a clear picture of your risk posture

Policies

Our Application Security Policy feature is the hallmark of our solution portfolio, and is used by all of our customers. We provide out-of-the-box policies for all of our different scan types, or you can create your own type of policy. When an application is scanned, its results are assessed against the chosen policy and, based on the results, determined to have passed or failed the set policy. From there, customers can do a number of things based on a passed/failed flag from the platform. For example, if they integrate with Jenkins, they can fail a build based on a failed policy scan.



A set of default recommended policies can immediately be leveraged, or an organization can customize their own based on their unique needs. The elements of an application security policy include:

- Types of flaws that should not be in the application (which are defined by flaw severity, flaw category, CWE, or common standards including OWASP, CWE/SANS Top 25, PCI, or CERT Secure Coding Standards).
- Minimum Veracode security score.
- Required scan types and frequencies.
- Grace period within which any policy-relevant flaws should be fixed.

Veracode also supports a functionality called "Custom Cleansers," which enables customers to mark their own custom-developed data validation libraries as trusted, so that Veracode will not mark data that passes through them as flaws. Additionally, if policies are changed, the compliance of an application can be assessed against the new policy rules without requiring a new scan.

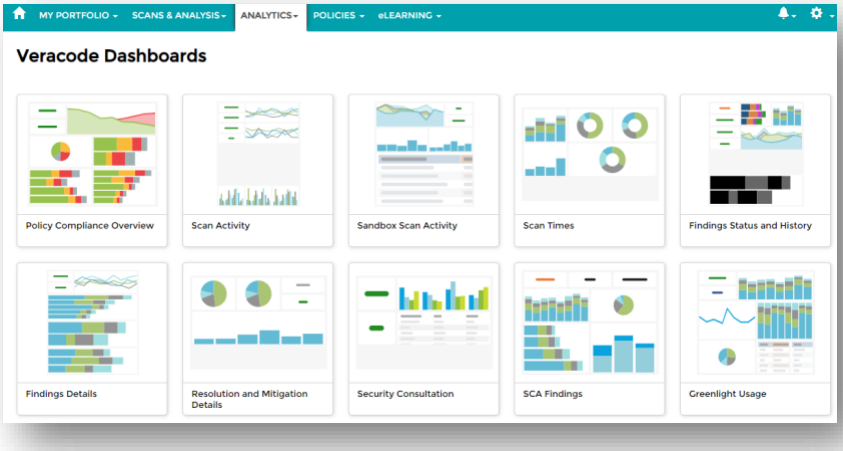
Analytics

There are hundreds of metrics are available for analysis in dashboards and custom reports in the Veracode Platform, such as:

- # of scans completed
- # of applications tested or not yet tested
- # of applications in compliance with policy or out of compliance
- # of vulnerabilities new since last scan
- # of vulnerabilities fixed
- # of vulnerabilities re-opened from an older scan
- # of vulnerabilities, net of approved mitigations
- # of vulnerabilities with proposed mitigations
- # of vulnerabilities with rejected mitigations
- Application size in MB (sum, average, min, max)
- Application size in LOC (sum, average, min, max)
- Application size in # of links crawled (sum, average, min, max)
- Flaws per MB (flaw density)
- Time to publish results in minutes
- Mean time to remediate

VERACODE

These metrics can all be reported on at the application, scan, or flaw level, or with respect to the time the scan completed. Application data includes business criticality and customer-specifiable metadata. Scan data includes the application language and dozens of other data points about the scan. Flaw data includes the CWE, category, and severity of the flaws found as well as the status of the flaw (new, reopened, fixed, mitigated etc.). We encourage customers to use this data to continuously improve their AppSec program. Examples of this include setting a mean time to remediate goal, as well as better understanding flaw categories that are most prevalent in order to provide targeted training and insights in compliance status.



Cover your entire application landscape with Veracode's language support

With more than 30 language releases and updates a year, our customers benefit from continuous additions to our supported languages to cover all of their current tech stack and future development work. For every language, our team is dedicated to maintaining a less than 1.1 percent developer-reported false positive rate for supported languages without manual tuning or customization work required.

Veracode supports more than 25 languages and 100 frameworks, including the following:

Languages and Platforms	Supported Versions
Java (Java SE, Java EE)	JDK and OpenJDK 1.3-1.9, 10, 11, 12 13
C#, VB.NET	.NET 1.0, 1.1, 2.0, 3.0, 3.5, 4.0, 4.5–4.8, .NET Core 1.0, 1.1, 2.0–2.2, 3.1, .NET Standard 2.0–2.1
ASP.NET with C# or VB.NET	.NET 1.x, 2.0, 3.x, 4.x / Core 1.1, 2.0–2.2
C++/CLI	.NET 2.0, 3.0, 3.5, 4.0, 4.5–4.8 (CLR 2.0)
JavaScript and TypeScript	ECMAScript 2015 and later
PHP	5.2–7.3
Scala	2.13
Groovy	2.4–2.6
Kotlin	1.3.x and earlier
Ruby on Rails	Ruby 1.9.3, 2.0.x, 2.1.x, 2.3–2.5, Rails 3.x, 4.x, 5.x

VERACODE

Apex	44.0 and earlier
PL/SQL	Oracle 18c and earlier
Classic ASP	Classic ASP 1.x, 2.x, 3.0
ColdFusion (compiled as Java)	ColdFusion 7, 8, 9, 10, 11
Perl	5.x (CGI Applications)
Python	2.x, 3.x
Go	1.x
Android	API Levels 8–28 (Android 2.2–9.x), API Level 29 (Android 10)
iOS	Xcode 9.x–11.3.x (LLVM)
Xamarin	Visual Studio 2012 and later/ Xamarin Studio/ Mono 4.x
PhoneGap/Cordova	PhoneGap or Cordova
Ionic	3.x-4.0
Titanium	Titanium SDK
React Native	0.50-0.54
C/C++ (Solaris 8, 9, 10 on SPARC)	gcc 3.3, 3.4, 4.0, 4.1
C/C++ (Red Hat Enterprise Linux 3, 4, 5, 6, 7 CentOS 3, 4, 5, 6, Fedora Core 6, OpenSUSE Linux 10, 11)	3.2-3.4, 4.0–4.9, 5.3–5.5, 6.3, 7.3
C/C++ (Windows)	Visual Studio .NET 2002–2017 (Visual C++ 7.0-14.1)
COBOL	Enterprise COBOL for z/OS, MicroFocus, ILE COBOL, COBOL-85, and ACUCOBOL-GT
RPG	RPG III, RPG IV, RPGLE
Visual Basic 6	Visual Basic 6

You can always find the latest up-to-date supported on our help center:
https://help.veracode.com/reader/wySvh2U7LWNYqeVS7PQm_g/x7GiAMwpmMWwMiENgHCwNw

VERACODE

Integrate Veracode into your tooling

Veracode provides extensive APIs, command line interfaces, plug-ins, and SDKs to allow customers to include static analysis into every phase of the application life cycle, including in development (IDE plugins), build or CI pipeline (build server plugins that can stop the pipeline if an application has significant security issues), workflow and orchestration, ticketing and bug tracking (defect tracking plugins), management reporting (GRC integrations), SAML, and more.

Background Knowledge

Integrating security is critical

Scanning more than 300 times per year increases your fix rate 3x and reduces security debt by 5x.

Veracode also has a repeatable on-boarding process for development teams that:

- Outlines specific application security goals for the team's SDLC
- Baselines the team's applications and provides remediation support
- Develops an SDLC integration strategy with the team to automate testing and results consumption
- Provides specialist integration support to help development, QA, and build teams leverage plug-ins, APIs and SDKs to instrument their SDLC

Enterprises that have leveraged our on-boarding process to integrate Veracode into their teams' SDLC test their applications much more frequently (typically 5x more).

Our out-of-the-box integrations include:

Developer IDE Plugins
Eclipse, IBM RAD
JetBrains InelliJ IDEA
Microsoft Visual Studio

Ticketing and Bug Tracking Tools
Rally Software
Atlassian JIRA
Microsoft Team Foundation Server (TFS)
Bugzilla
Micro Focus ALM
GitHub Issues

VERACODE

Build Systems
Jenkins
Microsoft Team Foundation Server (TFS)
Azure DevOps
Atlassian Bamboo
Apache Ant
Apache Maven
CA Continuous Delivery Director
JetBrains TeamCity
Gradle
CircleCI
CodeShip
Bitbucket Pipelines
Gitlab CI
Travis CI
Ansible*
Hygieia*

Web Application Firewalls (WAF)
Imperva SecureSphere Web Application Firewall
ModSecurity

GRC Systems
RSA Archer GRC
ThreadFix*
Kenna Security*

VERACODE

Workflow & Orchestration Tools
CA Automic

SAML Solutions
OKTA
PingOne
SAML Integrations for Veracode Platform

Below are examples of how each type of integration functions:

IDE Plugins: Before checking in code, developers can start a scan, review security findings, and triage the results of their Veracode Static Analysis scans all from within their IDE. In addition, developers can easily see which findings violate their security policy and view the data path and call stack information to understand how their code may be vulnerable to attack.

Ticketing & Bug Tracking: 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 not only create defect tickets, but they also automatically update or close them when the code is retested and the flaw is remediated.

CICD Systems (Build Systems): By integrating Veracode security testing into their build or release pipelines, Veracode customers can catch security issues as early as possible. Customers can test in the pipeline or in parallel, and can even break the build if security issues that violate policy are discovered.

Repositories: By integrating Veracode security testing into their binary repositories, customers can conduct one-time scans or scan binaries upon changes for security defects in first-party code.

GRC Systems: Veracode's GRC system integrations make it easier for customers to understand which applications may be in violation of their corporate security policies, and how quickly their organization is addressing issues.

Need to start Veracode scans or consume Veracode scan results from a different system? Veracode provides APIs that allow for full automation of the scanning lifecycle, consumption of results, and even provisioning and maintenance of Veracode platform user accounts. Our flexible APIs also allow you to create your own custom integrations or use community integrations, built by the open source community and other technology partners.

For a full list of integrations and their documentation, please visit:
https://community.veracode.com/s/integrations

VERACODE

Run an integrated DevSecOps program with Veracode

There are a number of different places where you could start your application security program, and many different paths to mature your program – but there are not many 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.