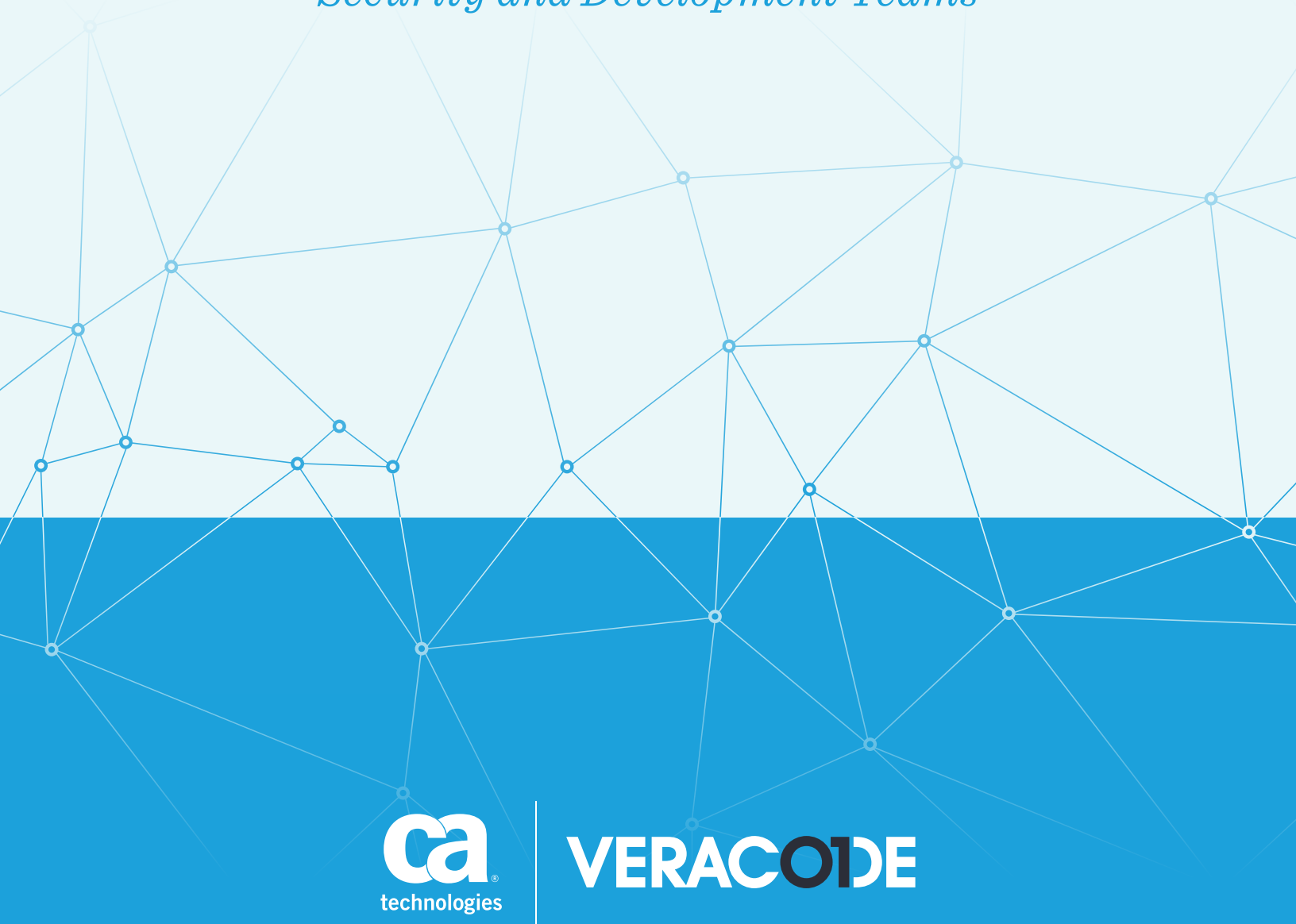
CA VERACODE INTEGRATIONS

Streamline Application Security for Both Security and Development Teams



ca technologies | VERACODE

As more organizations move to DevOps, application security (AppSec) solutions need to keep up or risk being left behind.

DevOps, a new organizational and cultural way of organizing development and IT operations work, combined with continuous integration and continuous deployment (CI/CD), have transformed the way we create software — making it a faster, more collaborative and incremental process. Even if you're just starting to think about DevOps, you know that the old way of doing software development is inadequate for meeting the demands on modern development teams, and eventually everyone will have to adopt the new model in order to compete.

To keep up with the shift to DevOps and rapid release cycles, application security solutions need to integrate into security and development teams' existing tools and processes as much as possible. Tacking additional steps onto the development process or forcing teams to interrupt their workflows to switch tools is becoming increasingly unfeasible within today's development paradigms.

In fact, AppSec tools that lack flexible APIs and customizable integrations will eventually be under-used, or not used at all.

Case Study

A cybersecurity company was struggling with developer security knowledge. Veracode helped train its team on Visual Studio and Eclipse plug-ins and helped them automate scans from a build server.

THEY WENT FROM PERFORMING

3–4 *scans per month*

↓

TO PERFORMING

60+ *scans in a four month period*

THEY'VE IDENTIFIED

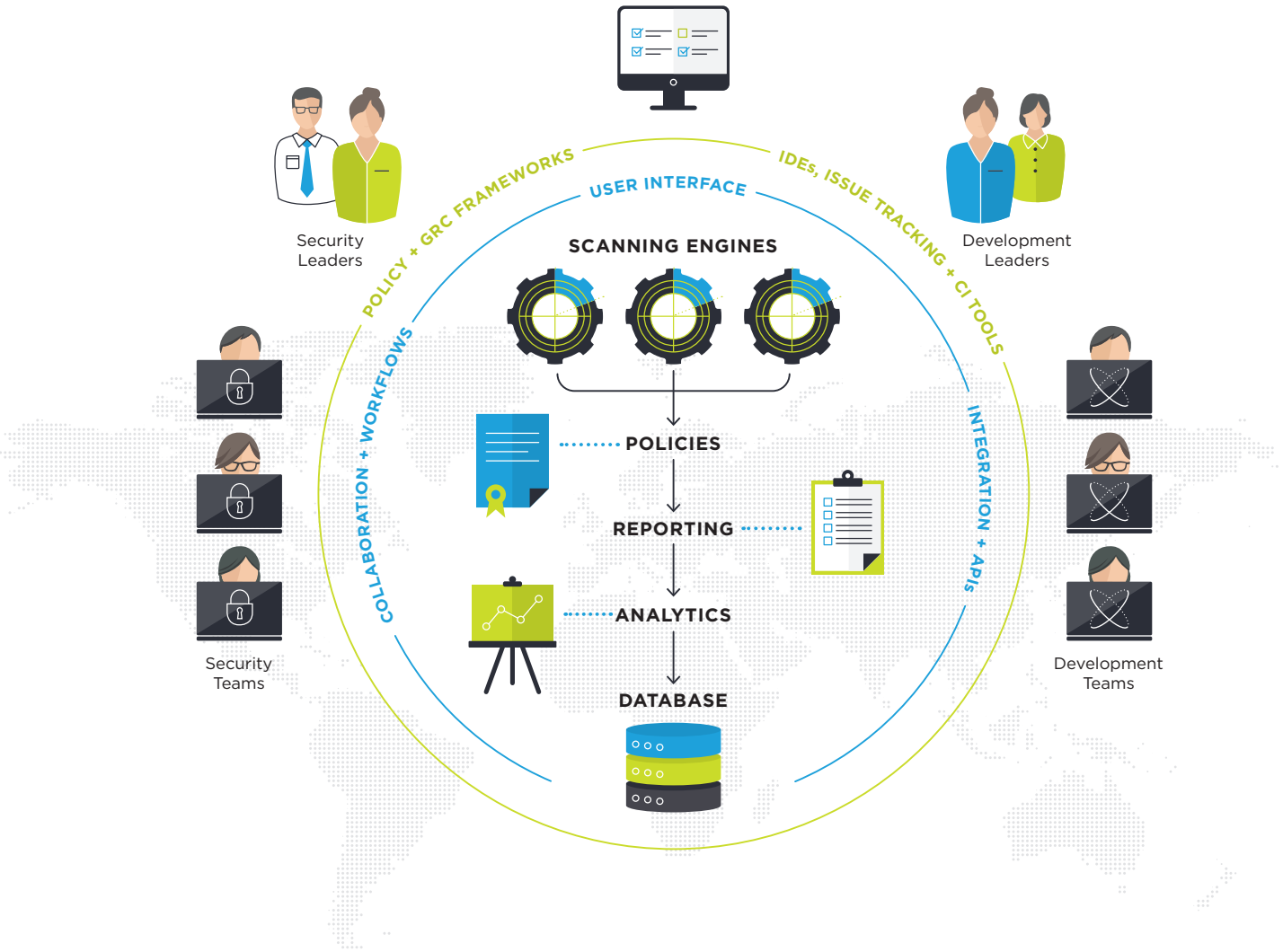
4,000+ *flaws*

↓

THEY'VE FIXED

25%+ *flaws in just four months*

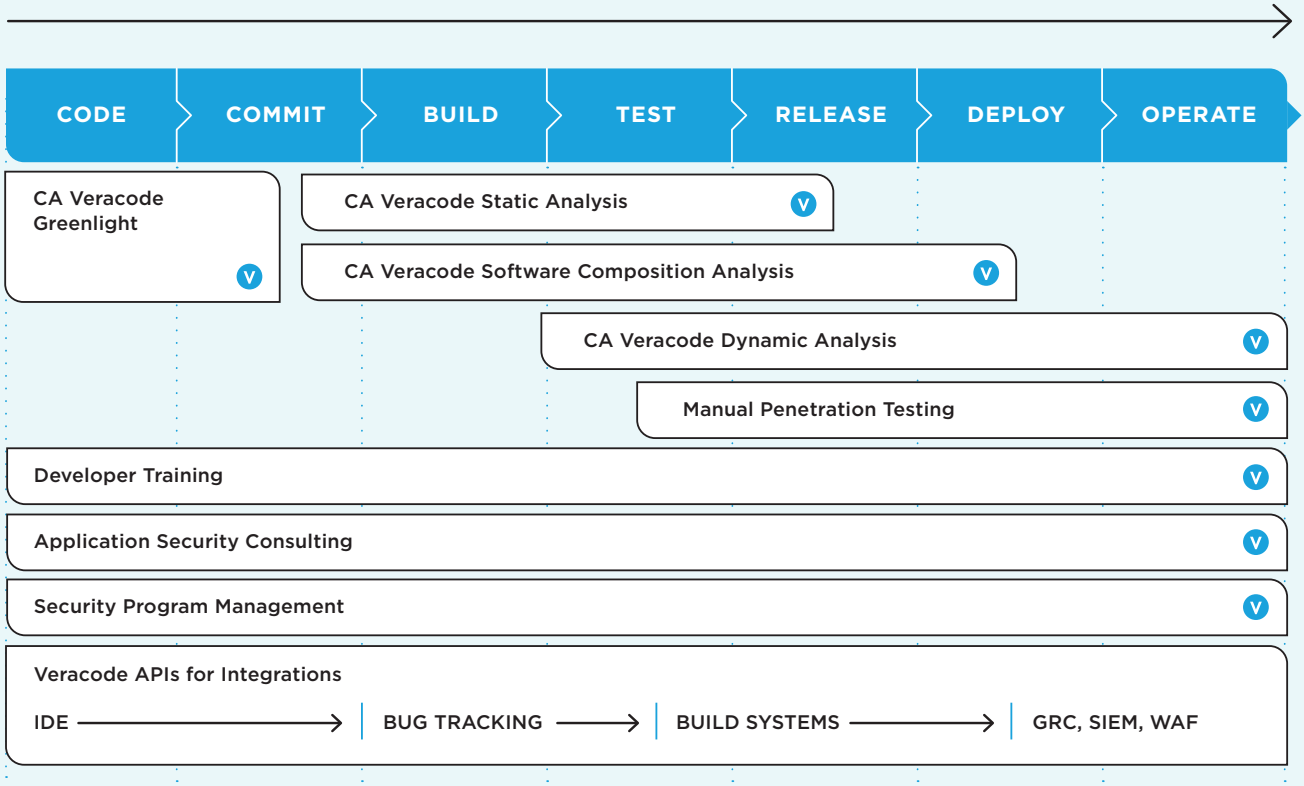
The Veracode Application Security Platform integrates seamlessly with the development, security and risk-tracking tools you already use. And, our flexible APIs allow you to create your own custom integrations or use community integrations, built by the open source community and other technology partners.



Read On

To get a better understanding of exactly how and where Veracode's solution integrates into the workflows of both developers and AppSec managers.

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



Integrating with the Development Team's Processes

Developers' processes might be changing, but their priorities are not. Although developers are now creating and testing code in smaller pieces more frequently and releasing updates more regularly, they remain focused on delivering quality code on tighter deadlines. Therefore, when it comes to security, their priority will be finding the line of code where a security-related defect is and getting information about how to fix it quickly. In addition, they have a particular set of tools and processes they use in order to create software and don't want to decrease their efficiency by having to switch gears.

Veracode's integrations work to keep developers meeting their goals in the face of changing development and security landscapes, to identify and address code vulnerabilities in their own development environment and using their own tools.

CA Veracode Integrates with Development Team's:

IDEs

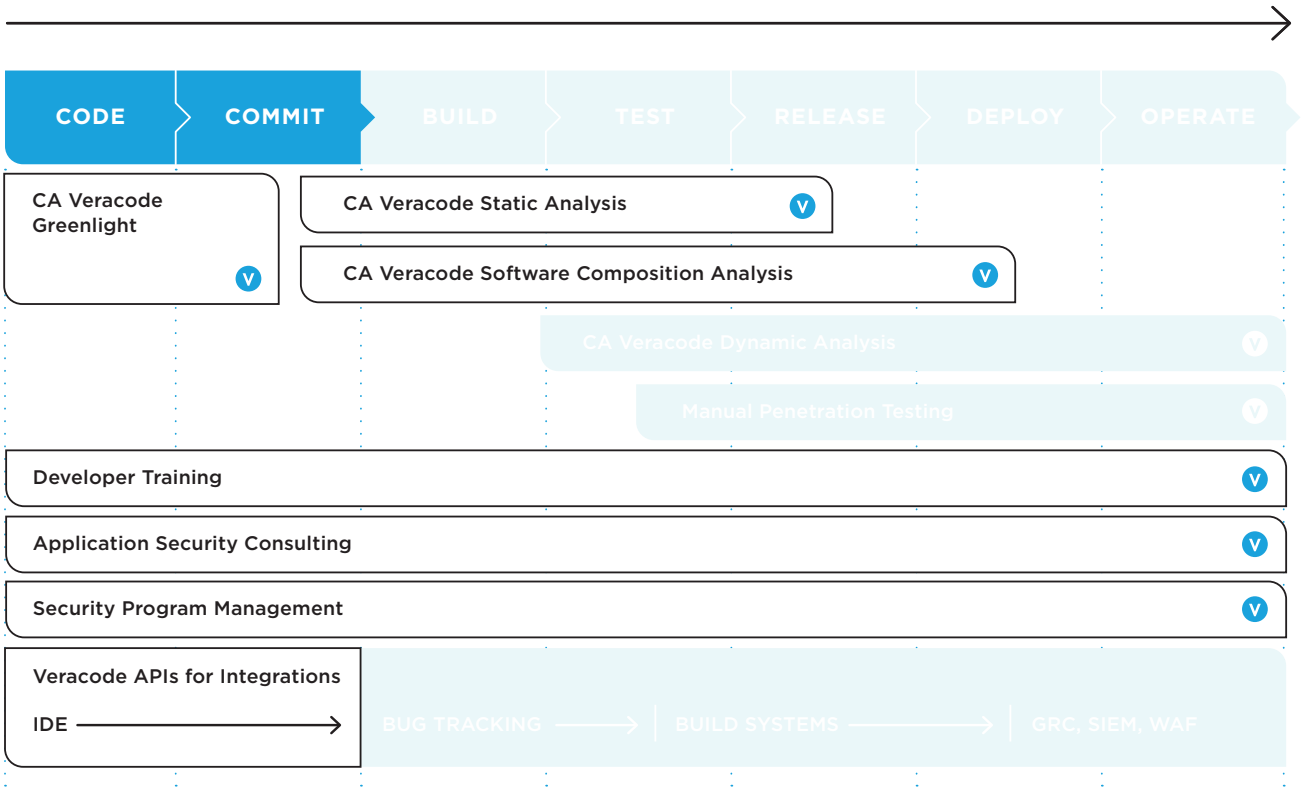
CA Veracode integrates with:

- Eclipse IBM RAD
- JetBrains IntelliJ IDEA
- Microsoft Visual Studio

With this integration, developers assess code for security and fix flaws — as they're writing it.

Veracode Greenlight allows developers to test individual classes as they work on them in their IDE, getting results back in seconds and highlighting areas where they've successfully applied secure coding principles.

Then, before checking in their code, developers can start a full application scan, review security findings and triage the results, all from within their own IDE. In addition, they 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.



Learn more

See first-hand how we integrate with your IDE, Get a personal demo of Greenlight.

Ticketing Systems

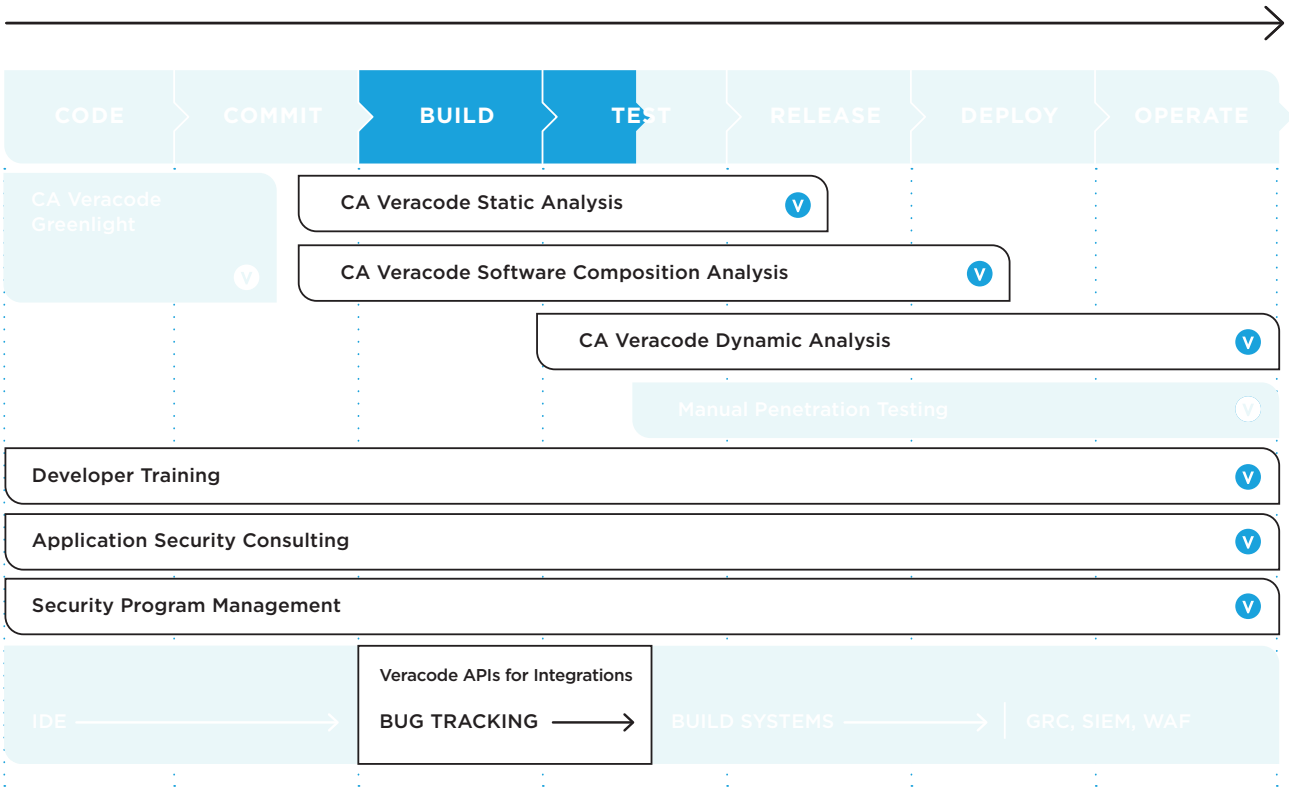
CA Veracode integrates with:

- Atlassian JIRA
- Microsoft Team Foundation Server
- Bugzilla
- HPE Application Lifecycle Management
- CA Agile Central

This integration enables Veracode's security findings to automatically appear as tickets in the developer's "to-do list." Based on scan results, the Veracode integration will open, update and close tickets related to security flaws automatically in developers' bug tracking systems, embedding Veracode scans into developers' work cycles.

When security flaws automatically pop up in their system as tickets, and then automatically close once they're fixed, developers save time because they don't have to go back and forth between Veracode and their ticketing system.

Each organization handles its ticketing process slightly differently, which is why Veracode offers flexibility in configuring the import process. You can import on a schedule or on-demand; associate tickets with distinct projects or import all security findings into the same place; map Veracode data fields into ticket fields; automatically label tickets; assign tickets to be fixed in certain releases; and more.



Learn more

Get your personal demo of CA Veracode Static Analysis

Build Systems

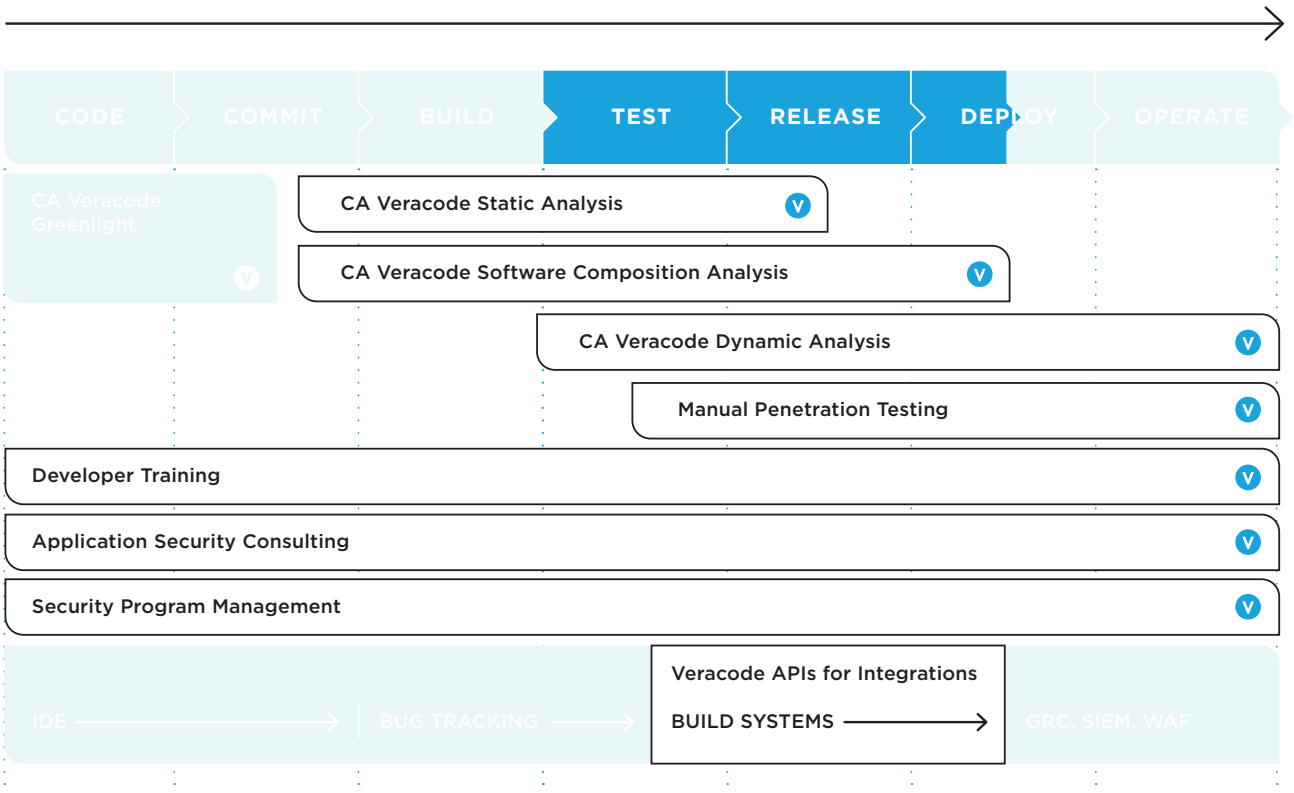
CA Veracode integrates with:

- Jenkins
- Microsoft Team Foundation Server
- Microsoft Visual Studio Team Services
- Atlassian Bamboo
- Apache Ant
- Apache Maven
- CA Continuous Delivery Director
- JetBrains TeamCity

With this integration, application security scanning is an automated step in the build or release process. Security testing simply becomes another automated test the build server performs, along with its other functionality and quality tests. Developers decide if an application should not be released if it does not pass Veracode policy.

If a security-related defect with a certain severity rating or prohibited open source component is found in the build process, this integration has the option to "break the build" and stop it automatically before code is released with these security issues. And with Veracode's low false-positive rate, breaking the build indicates a real vulnerability issue.

Veracode's build system integrations support integrating security testing both in stand-alone builds and as part of more complex pipelines. Depending on your team's needs, you can configure security testing with each build, within a release pipeline, or as part of a special security pipeline.



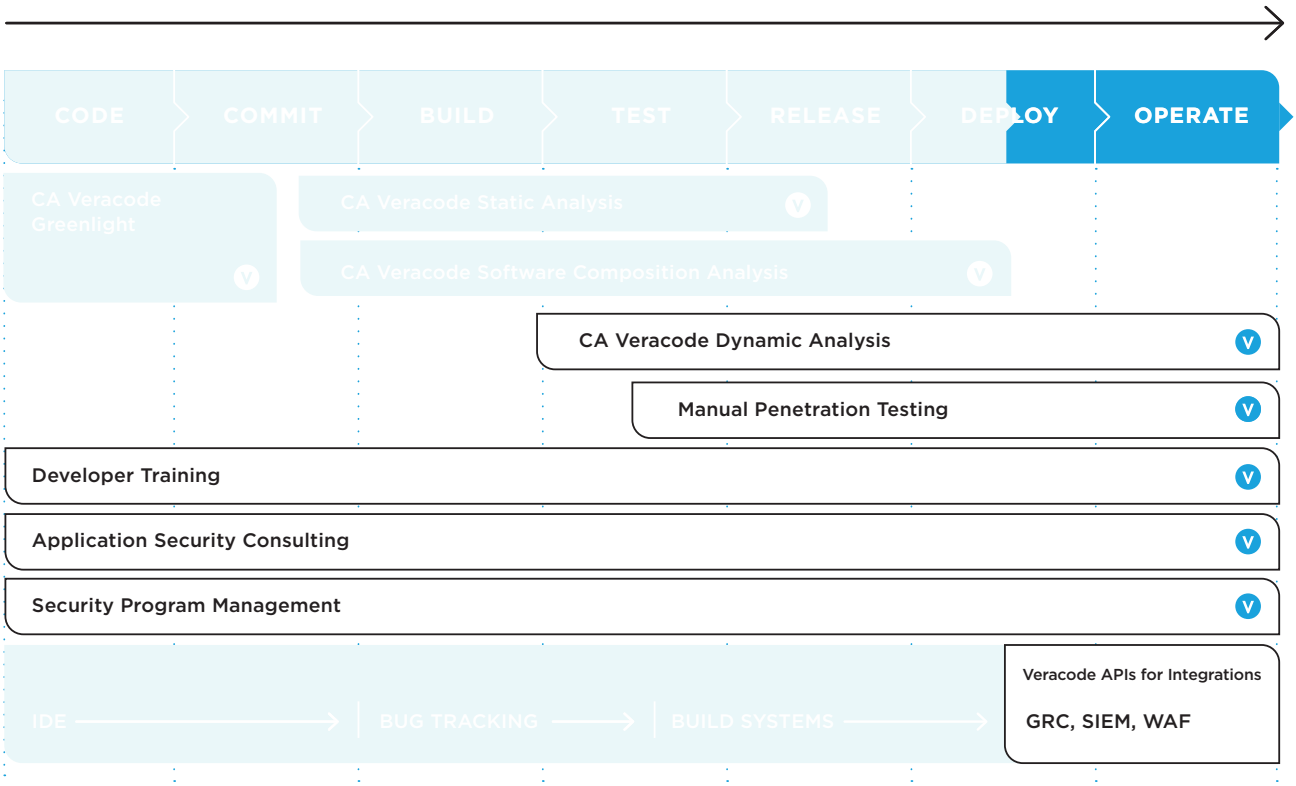
Learn more

Get your personal demo of CA Veracode Software Composition Analysis

Integrating with the Security Team's Processes

The security team is focused on reducing risk and achieving compliance, and needs to see reports about fix rates and compliance with regulations. From their perspective, data is the key to running an effective AppSec program. They need to be able to see trends so they can communicate priorities and progress, and gain the leverage they need to negotiate for business mindshare and budget.

Veracode's integrations feed data directly into the systems security professionals are already using, helping them to seamlessly get the data they need to better manage the AppSec program.



Veracode Integrates with Security Team's:

GRC Systems

By integrating with GRC systems, Veracode makes viewing and sharing data easier. We feed data into leading GRC platforms to share critical information such as:

- Application security scores
- Lists of all discovered flaws
- Flaw status information (new, open, fixed or re-opened)

Summary data is also included for third-party assessments, including scores and top-risk categories. In addition, we offer automated provisioning of new users and teams via APIs. Ultimately, this integration makes it simple for companies to track their application security compliance within the context of their corporate GRC initiative.

CA Veracode integrates with the RSA Archer GRC. 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.

Web Application Firewalls

Security professionals also need to maintain web application firewalls (WAFs), but managing large sets of blacklist rules can be challenging. Veracode simplifies this process by automatically generating blacklist rules for popular WAFs from dynamic scan data.

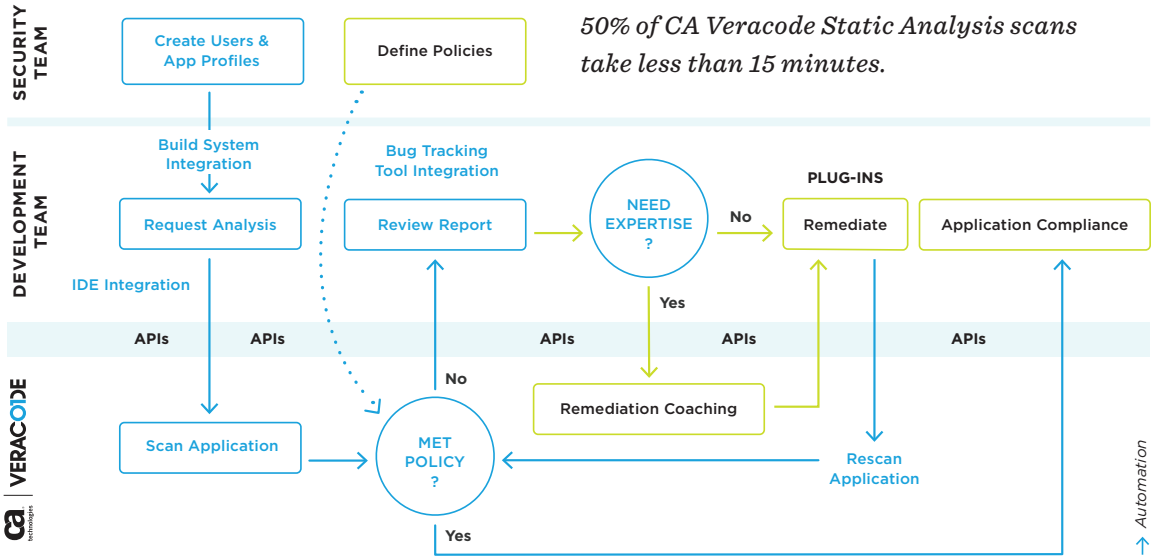
You can use Veracode dynamic scan findings to automatically generate rules for your web application firewall, so you can target just the problematic areas and block already-identified exploitable vulnerabilities in the application.

CA Veracode integrates with:

- Imperva SecureSphere Web Application Firewall
- ModSecurity

Integrate Securely

All Veracode integrations are built on top of the Veracode Application Security Platform, which provides common APIs and manages user access. Users can generate revocable API id/key pairs with built-in expiration dates to use these APIs, and individual API messages are secured via HMAC digest signing. And we protect your data the same way that we protect some of the largest corporations in the world, including banks, major manufacturers and government agencies.



50% of CA Veracode Static Analysis scans take less than 15 minutes.

Integrations Ease Friction

Veracode's integrations not only streamline the AppSec process for the security and development teams, but also help these teams work better together. With their differing priorities, it often seems like security and development teams are working at cross purposes. Veracode's integrations can ease some of that friction and help these teams work together toward the common goal of secure code.

For instance, when security isn't spending time manually kicking off scans and forwarding results, they can support more development teams, quicker, by focusing their time on building security into development processes.

In addition, Veracode's integrations give security increased visibility into both the status of their AppSec program, but also into what their application teams are struggling with, so that proper training can be provided. For instance, with the GRC system integration, an AppSec manager could quickly and easily see if one particular dev team is producing code with more SQL injection flaws than other teams. The AppSec manager can then provide the right type of training to the right people.

Conclusion

***Software development** is changing, and **software security** needs to change along with it.*

Application security solutions that force developers or security professionals to switch gears and slow their processes are no longer relevant. Application security today needs to blend seamlessly with the tools and processes these teams are already using, and Veracode's integrations are an important part of that requirement.

See For Yourself

Take a guided tour through our solution; get your personal demo of the CA Veracode Application Security Platform.

Veracode, CA Technologies' application security business, is a leader in helping organizations secure the software that powers their world. Veracode's SaaS platform and integrated solutions help security teams and software developers find and fix security-related defects at all points in the software development lifecycle, before they can be exploited by hackers. Our complete set of offerings help customers reduce the risk of data breaches, increase the speed of secure software delivery, meet compliance requirements, and cost effectively secure their software assets — whether that's software they make, buy or sell. Veracode serves over a thousand customers across a wide range of industries, including nearly one-third of the Fortune 100, three of the top four U.S. commercial banks and more than 20 of the Forbes 100 Most Valuable Brands.

Learn more at veracode.com, on the Veracode Blog, and on Twitter.