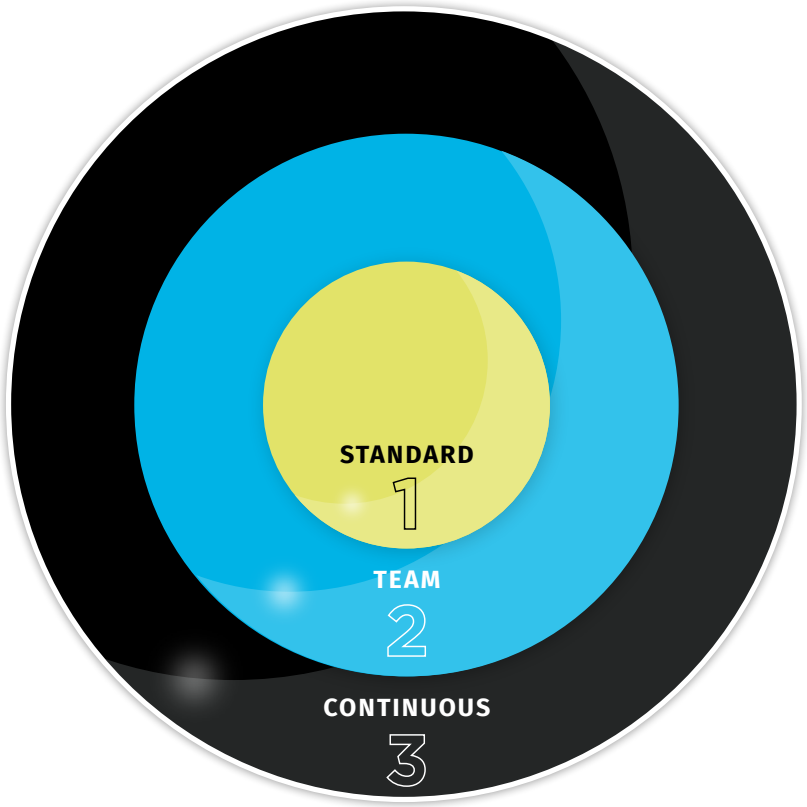
Turn the Benefits of Veracode Into a Competitive Advantage With Veracode Verified™



VERACODE VERIFIED™ DEFINED

Veracode Verified provides attestation that a development team has a framework in place to assess the security of an identified application. The three tiers of the Veracode Verified™ program deliver code-level security for applications while driving process maturity for an application security program.

For more information about how Veracode can promote innovation within your enterprise, visit the Veracode website.

SECURITY MUST OCCUR AT DEVOPS SPEED

You can't afford to have developers slowed by a need to constantly switch tools and tasks. You also can't afford to ship insecure code that leaves you and your customers at risk for a breach.

INTEGRATE TO INNOVATE

Veracode offers tools and solutions that integrate with your existing security and development frameworks and automate processes, letting you ship secure code faster. These tools and solutions can help you establish a superior application security environment, and they put your development teams at the center of testing. They integrate with your:

- **IDEs.** Start a scan, review security findings and triage the results, all from within your IDE.
- **Build systems.** Test in the pipeline or in parallel.
- **Ticketing systems.** Automate the creation, updating and closing of defective tickets.
- **GRC systems.** Veracode provides native integration for RSA Archer.

In addition, 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.

AUTOMATION IS KING

Getting features to market quickly and securely means taking humans out of the equation as much as possible. Veracode automates security testing tasks throughout the development process. For instance, with Veracode's build system 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 functionality and quality tests.

Another example is Veracode's integration with ticketing systems, which 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.

Give your customers confidence that your software is secure … make sure it's Veracode Verified.™

You're making security a priority and working to deliver high-quality, secure code — now prove it!

The Veracode Verified™ program allows your organization to stay in front of prospect security concerns — thus speeding your sales cycle. It demonstrates your organization's unwavering commitment to application security through third-party measurement and attestation tools that demonstrate progress — and results. With Veracode Verified,™ your security program is backed by one of the most trusted names in the industry.

CUSTOMER VALUE

↑ Revenue:

- Accelerated sales cycles by demonstrating to the software buyer that your organization has made security a priority

↓ Cost:

- Unburden the security team by eliminating the additional time required to respond to increasing annual security audits
- Reduced costs of fixing flaws once the application is in production by integrating security assessments earlier in the software development process. Development can remediate flaws earlier in the cycle

↓ Risk:

- Reduction in the false sense of security of attestation letters, which only provide a point in time view into the security of an application. Each level of the Veracode Verified program is iterative and the policy applied to the application enforces the continued compliance to the level achieved
- Decreased number of flaws introduced or re-introduced into software by arming development teams with a Security Champion
- Increased visibility into the risk-level of the software your organization is acquiring
- Reduction of risk introduced into your business environment through the 3rd-party supply chain. Allow the Veracode Verified program to simplify the security evaluation of these applications by requiring software vendors comply with the appropriate Verified level

Ready to get Veracode Verified™?

Here are the steps you need to take to achieve the highest Veracode Verified™ level: Verified Continuous.

1 Verified **Standard**

At this tier, your organization:

- Assesses first-party code using static analysis.
- Documents that applications don't allow Very High flaws in first-party code.
- Establish a scanning cadence of at least every six months.
- Provides developers with remediation guidance.

Veracode customers that offer developers remediation coaching improve fix rates by 88 percent.

Are you applications Veracode Verified™?

Find out more and get started by visiting https://info.veracode.com/contact-us-verified-program.html.

2 Verified **Team**

This tier includes all the elements of Verified Standard, plus:

- Document that an application doesn't include Very High or High flaws, and that you have a 60-day remediation grace period to remain in compliance.
- Establish a scanning cadence of at least every 90 days.
- Identify a security champion within the development team to serve as a peer resource to development team members, ensuring secure coding practices across the development lifecycle.
- Provide training or labs on secure coding for the identified security champion.
- Assess open source components for improved security, and document that they don't contain any Very High or High vulnerabilities.
- Provide developers with remediation guidance for both 1st party code flaws and open source vulnerabilities.

A DevSecOps development model where scans average *over 260 a year have a fix rate of 19 days, which is 3.5x greater* than applications scanned less than 12x.

3 Verified **Continuous**

This tier encompasses all the elements of Verified Team, plus:

- Integrate security tools into development workflows.
- Complete a post-product security assessment (dynamic analysis or penetration testing).
- Document that your applications don't include any Very High, High, or Medium flaws.
- Undergo Veracode's biannual mitigation review as well as a 30-day remediation grace period to remain in compliance.
- Provide advanced training or labs on secure coding for security champions.
- Establish a scanning cadence of at least every 60 days.
- Provide development teams with training or labs on secure coding.
- Assess open source components for security, and document that open source components don't contain Medium, High, or Very High vulnerabilities.

Veracode's *State of Software Security* report found that organizations with long-standing, comprehensive AppSec programs had a 35 percent better OWASP pass rate than those with programs in place for a year or less.

VERACODE