

# Veracode SDLC SecurityReview®

## Highlights

### Enterprises use SDLC SecurityReview To:

- Determine if software is secure to release or ship
- Independently verify and validate the security of software in its final form
- Shorten time to market & reduce costs
- Increase and expand security testing without additional resources
- Market software security as a competitive differentiator

### Key Features:

- **Automated & On-Demand** – Application security testing on an as-needed basis
- **Security-as-a-Service (SaaS)** – Lower costs with no hardware or software to purchase, install & maintain
- **Integrated Technology** – Allows companies to do more with less by combining static and dynamic testing – equivalent to getting two “tool” products plus security expertise in a single subscription
- **Independent Standards-Based Ratings** – Ratings based on NIST, CWE & CVSS to meet auditing & compliance standards
- **Rapid Time to Value** – Actionable results available within 24-72 hours

Whether you are a software vendor or developing software for internal use, you need to ensure that your applications are secure. Veracode SDLC SecurityReview provides enterprises with the ability to conduct security assessments on applications before they ship or are deployed via a simple, cost effective, on-demand subscription service. Based on breakthrough binary analysis, Veracode independently verifies the security posture of applications within 24-72 hours without requiring any additional hardware, software or personnel.

### The State of Application Security

Application security has risen to the top of the agenda for security professionals striving to control their company’s overall risk profile. According to Gartner and the Computer Emergency Response Team (CERT), 75% of new attacks target the application layer and software vulnerabilities have reached an all time high – with more than 7,000 new vulnerabilities discovered over the last year.

As the myriad of applications developed and deployed increases, the effort needed to manage risk becomes greater. Applications are inherently more complex – with many being based on a mixed code base from a wide range of sources, teams, and geographic locations. Gone are the days when companies developed 100% their own source code. A large percentage of organizations contract at least some phases of their development. Software vendors and enterprises have lacked an effective manner to evaluate the complete security quality of their applications as part of the release or deployment process. Traditional tools alone cannot rise to this challenge as they typically require source code which usually isn’t available in mixed code based applications and do not examine the application in its final, assembled form. Manual penetration testing is time consuming, costly and simply doesn’t scale. Veracode was specifically created to address these challenges.

### Independent Security Audit before You Ship

Protect your customers by using the world’s first on-demand security health check on your software before you ship. Veracode enables enterprises to conduct security audits by an independent trusted entity on the final application code as part of an organization’s formal software release process, without the need for specialized tools, additional hires or costly on-site consultants. Simply configure an assessment using Veracode’s On-Demand Assurance Platform and receive expert results within 24 to 72 hours with detailed remediation information. Veracode’s Software Assurance Report gives managers the information and insight they need to determine if software is ready to ship or deploy into production.



In a NY Times article Mr. Feiman called Veracode’s service to test binary code a “Breakthrough”

**Joseph Feiman**  
VP & Gartner Fellow

### Enterprise Benefits

#### Speed Remediation Veracode Fix First Analysis



Veracode's Fix First Analysis quickly identifies flaws and guides your developers through remediation efforts

#### Compliance Milestones



Veracode's On-Demand Service tracks your application's ratings over time, enabling you to improve your project milestones



#### Deliver Business Value: Do More With Less

In today's trying economic times, organizations need to cut costs while providing a higher level of service. Veracode's unique combination of automation, on-demand delivery and integrated technology enables businesses to increase their security without adding full time resources or purchasing expensive hardware or software. With security expertise in short supply, Veracode's allows companies to improve the productivity of their existing resources and security investments through automation. The combination of static binary analysis and dynamic web scanning in a single service is equivalent to purchasing two separate products and our on-demand subscription service allows enterprise to scale testing on an as-needed basis without large capital and operational investments.

#### Leverage Standards-Based Security Ratings

As an independent and trusted provider of automated security ratings, Veracode can conduct a security assessment more successfully without any bias, ensuring oversight and a clear audit trail to meet both internal security best practices as well as formal regulatory compliance initiatives. Veracode is the only solution is based on a standards-based scoring system that leverages MITRE's Common Weakness Enumeration (CWE) for classification of software weaknesses and FIRST's Common Vulnerability Scoring System (CVSS) for severity and ease of exploitability and NIST for assurance levels. These universally accepted vulnerability scoring methods provide a set of clear metrics which enterprises use to set security thresholds into release and deployment processes.

#### Promote your Security as a Differentiator

Whether you are a software vendor or developing applications for internal use, your customers need to know that your applications are secure. The Verified by Veracode Program is quality indicator for the security level of applications and software components. The program provides visible proof that your application was rigorously tested against industry-standard benchmarks. End-users and enterprises gain insight into the security quality of software similar to that provided by Moody's®, Standard and Poor's® for financial markets or Consumer Reports® for other products. Enterprises use this information to demonstrate compliance with internal auditing or external regulatory requirements while software vendors can now market the security of their software as a competitive differentiator.

#### About Veracode

Veracode is the world's leader for on-demand application security testing solutions. Veracode SecurityReview is the industry's first solution to use patented binary code analysis and dynamic web analysis to uniquely assess any application security threats including vulnerabilities and malicious code. SecurityReview performs the only complete and independent security audit across any internally developed applications, third-party commercial off-the-shelf software and offshore code without exposing a company's source code. Delivered as an on-demand service, Veracode delivers the simplest and most-cost effective way to implement security best practices, reduce operational cost and achieve compliance without requiring any hardware, software or training.

Veracode has established a position as the market visionary and leader with awards that include recognition as a Gartner 'Cool Vendor' 2008, Info Security "Tomorrow's Technology Today Award 2008", Information Security "Readers' Choice Award 2008", AlwaysOn Northeast Top 100 Private Company 2008, NetworkWorld "Top 10 Security Company to Watch 2007", and Dark Reading's "Top 10 Hot Security Startups 2007". Based in Burlington, Mass., Veracode is backed by .406 Ventures, Atlas Venture and Polaris Venture Partners. [www.veracode.com](http://www.veracode.com). For more information, visit [www.veracode.com](http://www.veracode.com)