

Application Risk Management Solutions



Your world runs on applications.  
Secure them with Veracode.

**VERACODE**  
*Software Security Simplified*



Application security risk is inherent in every organization that relies on software to run its business. Today's applications control access to Personally Identifiable Information (PII), Personal Health Information (PHI) and financial data transactions, and have become the enterprise's "new perimeter." With challenging economic times and a tightening risk and compliance environment, businesses are required to do more with less and need a better approach to secure their software and protect their business with existing budgets.

Whether you are developing software, using open source applications, leveraging COTS or working with outsourcers, your exposure to security risks and vulnerabilities puts your customers and your bottom line at risk. The security of your brand and your customer data will determine whether your applications are your greatest assets or potential liabilities.

## US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

"90% of security incidents result from exploits against defects in software"

How do you plan to manage application risk?

# SecurityReview®

## SecurityReview® Highlights

### Application Risk Management Platform

Leverage a centralized view of risk and security information to manage, track and report on your application portfolio across your entire enterprise; available 24x7 through Veracode's secure, web-based SaaS platform hosted in a secure Software Assurance Center.

### Automated Code Review

Veracode's patented automated static binary analysis reviews code in its "final" compiled version, including libraries and 3rd party components, without requiring organizations to expose their intellectual property in the form of source code. This approach results in the most accurate and complete security testing available in the industry.

### Automated Web Vulnerability Scanning

Veracode's automated web application vulnerability scanning, also known as dynamic analysis or black-box testing, empowers companies to identify and remediate security issues in their web applications before hackers can exploit them.

### eLearning

SecurityReview integrates web-based secure programming training modules for developers and security personnel to meet formal training and competency testing requirements.

### Open Source Ratings Database

Veracode's database of security ratings for enterprise-class open source projects enables organizational understanding of the risk/benefit trade-off of integrating open source versus commercial software.

### Custom Policies and Compliance Management

Veracode's risk-management platform allows organizations to meet the application security requirements of PCI, OCC Bulletin 2008-16, FISMA, HIPAA, SOX, GLBA and industry standards such as, OWASP Top 10 and SANS Top 25, by setting security policies for assessments.

### Security Advisor Services

Leading enterprises leverage Veracode's full range of application lifecycle services including application inventory support, remediation advice, build and upload support, and program management services.

Veracode is the world's first provider of Application Risk Management solutions. Veracode's award-winning SecurityReview® service provides centralized governance and control for comprehensive, cost-effective software security assessments, as well as training and compliance management for your entire application portfolio.

Enterprises, ISVs and government agencies are leveraging SecurityReview today to quantify and manage the security risks of internally developed, commercial, outsourced and open source applications, before they are shipped to customers or deployed in-house. SecurityReview enables organizations large and small to implement a best practices framework and solution platform for managing application risk across your enterprise.

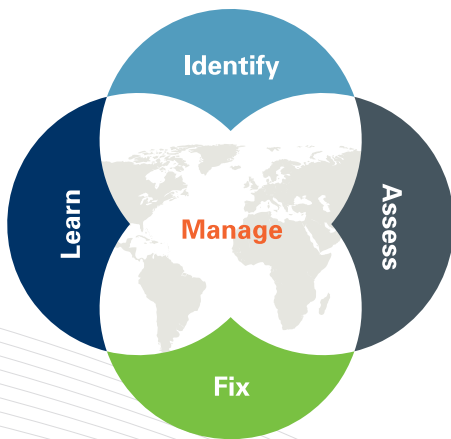


“Veracode’s existing technology solutions for testing application binaries without requiring access to source code is crucial for any organization that brings externally developed software in-house.”

In-Q-Tel

# Comprehensive Control of Application Risk

SecurityReview® empowers organizations to transform application disorder into a standardized best practices framework for application risk management. The single portal normalizes the view of critical applications and provides a reliable, cost-effective and centralized view of application security risk. Using a simple framework –Identify–Assess–Fix–Learn–Manage–the SecurityReview console and testing platform brings together key process information and assessment metrics across security and development organizations. This facilitates a productive dialogue between developers, managers and executives, and supports informed business decision-making about the acceptable security risk for your enterprise.



Veracode SecurityReview®

## Identify

Define and classify your application portfolio.

- Select applications and assign or import meta data according to origin, type and development team
- Classify business criticality based on regulatory and business impact
- Set security policy based on market standards—SANS Top 25, OWASP Top 10, Veracode Security Ratings

## Assess

Scan and verify code for security vulnerabilities that matter most.

- Schedule the security tests appropriate for your application based on business criticality
- Perform automated scanning (static, dynamic) and manual testing
- Leverage binary static analysis to find vulnerabilities source code won't reveal, such as backdoors and malicious code

## Manage

Manage your entire application portfolio's security risk from a single dashboard.

- Track the progress of software assessments, review remediation activities, prioritize fixes
- Organize information of highest value to CISOs, business application owners and development managers
- Support informed decision-making through better intelligence on your application risk, whether built or inherited

## Fix

Review a comprehensive snapshot of your application risk to find and fix problems quickly.

- Remediate based on a concise and prioritized list of applications and vulnerabilities which pose the highest risk
- Remediate direct to line-of-code for faster results
- Maximize productivity due to SecurityReview's industry leading low false positive rates

## Learn

Access eLearning modules to provide developer education and improved security.

- Measure developer eLearning progress by individual or application
- Leverage embedded eLearning modules to provide focused courses on SANS Top 25, OWASP Top 10 and other industry standards
- Learn about security vulnerabilities inherited from open source applications



# Best Practice and Best Fit

SecurityReview®'s flexibility allows organizations and users to pick the most effective set of best practices to facilitate their application security requirements.

## CISOs and CIOs

Security executives and information officers can set policy, quickly review the state of the application portfolio and identify which applications are out of compliance, for both internally development and third party applications.

- Specify policy through a centralized console across the application portfolio
- Manage application policy conformance
- Govern the security quality of outsourced code providers to ensure acceptance standards are met
- Manage security review and verification for custom code prior to deployment
- Normalize security assessment metrics across multiple code sources for consistent reporting

## Security and Audit Professionals

Security and audit professionals can test applications prior to final acceptance or when an audit event is triggered for existing and deployed applications.

- Manage sensitivity classification of applications based on source, type of data, and architectural placement
- Review test metrics across all units and divisions
- Report on policy conformance prior to deployment or post-deployment
- Identify at-risk applications and recommend compensating controls
- Implement board-level policy related to data leakage, privacy and customer information, effectively

## Developers

Development teams can spend less time worrying about code compliance and more time getting verified applications into production quickly. SecurityReview enables rapid identification of coding problems while delivering the lowest false positives rates in the industry along with easy-to-understand fix recommendations.

- Accelerate the security review process—quickly identify and fix problems before the auditor assessment
- Test code repeatedly throughout the development process, before final check-in, or both
- Direct to line-of-code recommendations for rapid remediation and increased productivity

**“In a rapidly changing threat environment, Veracode’s technology and it’s software-as-a-service model have given us the flexibility to conduct rapid code review cycles, which is an obvious benefit for our customers”**

Rhonda MacLean  
CISO of Barclays

# Software Security Simplified

Veracode SecurityReview® solutions are delivered as flexible services that can be customized to fit your enterprise's unique needs and accommodate the changing threat and security requirements' landscape as your business grows.



SecurityReview® Solutions	Standard Edition	Enterprise Edition
Application Portfolio Dashboard	✓	✓
Automated Code Review (Static)	✓	✓
Automated Web Vulnerability Scanning (Dynamic)	✓	✓
Enhanced Dynamic Application Security Testing	✓	✓
Open Source Ratings Database	✓	✓
Executive, Manager & Developer Reports	✓	✓
Customer Support	✓	✓
Designated Customer Support Contact (TAM)		✓
Security Program Advisor Hours		✓
Developer Security Certification		✓
eLearning		✓
API/Archer Integration		✓
Co-Branding		✓

## VERACODE

Veracode, Inc.  
4 Van de Graaff Drive  
Burlington, MA 01803

Tel +1.781.425.6040  
Fax +1.781.425.6039

www.veracode.com

ARMS/0909

### ABOUT VERACODE

Veracode is the world's leader for cloud-based application risk management solutions. Veracode SecurityReview is the industry's first solution to use patented binary code analysis and dynamic web assessments combined with developer e-learning and access to open source security ratings to independently access and manage application risk across internally developed applications, third-party commercial off-the-shelf software and offshore code without exposing a company's source code. Delivered as a cloud-based service, Veracode provides the simplest and most-cost effective way to implement security best practices, reduce operational cost and achieve regulatory compliance with requirements such as OWASP, SANS Top 25 and PCI compliance without requiring any hardware, software or training.