

# VERACODE

SOLUTION FACT SHEET

## Highlights

### Enterprises use Third-Party SecurityReview

- Establish Secure Procurement Initiatives
- Evaluate vendors as part of the RFP process
- Set minimum security thresholds for purchased software
- Understand risks in mergers and acquisitions

## Key Differentiators

- **Archer-Veracode Integration:** Allows companies to integrate Veracode's application risk management and software vulnerability results into their overall Archer GRC solutions
- **No Source Code Required:** The source code of commercial software is rarely available for testing. For the first time, organizations can test the software by using Veracode's patented binary analysis
- **Cloud-based delivery:** Lower costs with no hardware or software to purchase, install and maintain
- **Integrated Technology:** Allows companies to do more with less by combining static and dynamic testing plus program management expertise in a single subscription
- **Independent Standards-Based Verification:** VerAfied mark provides independent verification based on industry standards derived from NIST, CWE & CVSS to meet auditing and compliance requirement

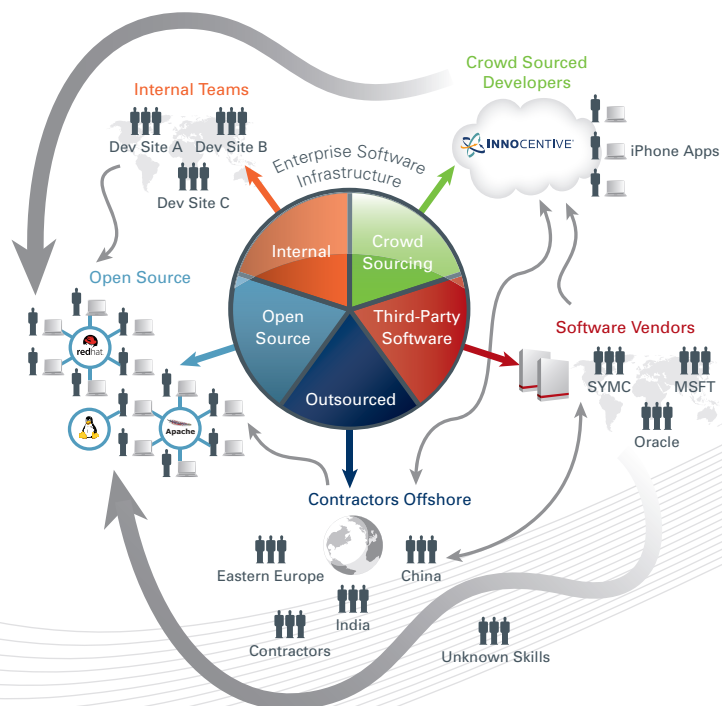
## Third-Party SecurityReview™

Veracode's State of Software Security report indicates that between 30% and 70% of applications classified as internally developed are actually comprised of third-party libraries and components. Veracode's Third-Party SecurityReview helps quantify and manage security risks from third-party applications in a cost-effective and scalable manner.

## Complex Software Value Chains Increase Risks

It is imperative for organizations to manage risk from applications procured through the extended software supply chain of commercial, outsourced or offshore software providers. Traditional testing techniques such as source code scanning are not a viable option for verifying third-party applications or components due to lack of access to source code (software vendor intellectual property). Automated black box tests using dynamic scanning tools are restricted to Web applications only and cannot assess back-office components and n-tier applications. Manual penetration tests are time consuming, costly and do not scale.

As a result, enterprises either do not test third-party applications at all or are restricted to analyzing a small subset of their purchased software which is insufficient to adequately manage risk.



## Benefits

### Enterprise Benefits

- Minimize unbounded risk associated with third-party software and service providers
- Transfer management overhead of managing third-parties to Veracode
- Gain Independent verification of security quality of third-party applications before they become part of your software infrastructure
- Develop a secure procurement governance model that delivers permanent and persistent success for the business

### Vendor Benefits

- Obtain detailed insight into the security risk of software products they are bringing to market (without parting with intellectual property)
- Proactively execute actionable remediation recommendations to improve security quality for their customer base
- Leverage Veracode's VerAfied mark to differentiate competitively and market security as a key feature and selling point



“Not having binaries tested leaves in a gap in application security. Veracode aims at covering the gap.”

JOSEPH FEIMAN  
VP and Gartner Fellow

**VERACODE**  
Software Security Simplified

Veracode, Inc.  
4 Van de Graaff Drive  
Burlington, MA 01803  
Tel +1.781.425.6040  
Fax +1.781.425.6039  
www.veracode.com

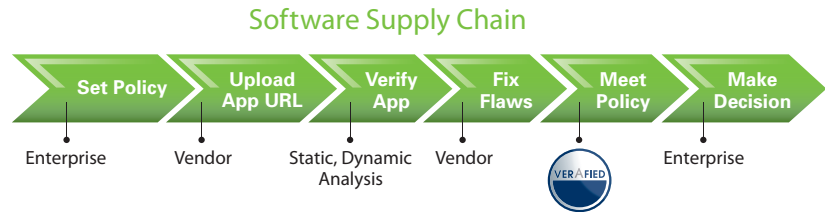
© 2010 Veracode, Inc.  
All rights reserved.

SFS/TP/2010

## Binary Changes the Game: Third-Party SecurityReview

Veracode's Third-Party SecurityReview service makes it simple and cost-effective to assess risk from the extended software supply chain. Veracode is the world's only vendor that can inspect software executables (binary or bytecode) without asking vendors to expose any of their intellectual property in the form of source code. Veracode's patented technology analyzes the binary or bytecode which is the truest representation of the final application.

Enterprises set the security policy for the application. Software suppliers simply upload the binary or bytecode to the cloud-based platform and Veracode performs an independent standards based verification and provides summary results to the enterprise and detailed results to the Software IP owner to help them mitigate identified vulnerabilities and achieve compliance.



Key features of Veracode's Third-Party SecurityReview:

- **Unlimited Vendor Applications:** Assess an unlimited number of vendor applications. An assessment consists of a static analysis or dynamic analysis scan with allowance for remediation scans as needed to achieve compliance with the enterprise policy. Vendor applications found to be in compliance with Veracode's VerAfied program criteria will also be eligible for earning the VerAfied security mark and placement in Veracode's VerAfied vendor software directory.
- **Unlimited Users:** The service allows for an unlimited number of users to be provisioned on the cloud-based platform for either the enterprise or the vendor.
- **Application Portfolio Dashboard:** Access a centralized view of risk and security information to manage, set policy, track and report on all Third-Party software vendors.
- **Open Source Ratings Database:** Gain access to Veracode's database of security scores for commonly used open source projects enabling an understanding of the risk/benefit trade-off of integrating open source versus commercially developed software.
- **Enterprise Summary Reports, Vendor Detailed Reports:** In order to respect intellectual property ownership detailed findings are only made available to the Third-Party vendor and a high-level summary report to the enterprise with enough information on the application's performance for the enterprise to make a purchase or acceptance decision.
- **Extensible, Open Platform:** Enterprises can also benefit from automated integration with Archer's GRC Framework product to obtain a centralized view of vendor policies and compliance. For the software vendor it offers xml exports and a results api that can be used to integrate findings with tools that typically form part of the SDLC such as bug and defect tracking systems.

Some subscription levels include enhanced program management services by including a half-time customer success manager (CSM). The CSMs kick-off the engagement by conducting a workshop to develop the policies and program framework for on-going governance. They also help to on-board vendors and manage the testing and acceptance process on an on-going basis relieving the enterprise from the management overhead of dealing with multiple third-parties.

All Third-Party SecurityReview customers also get access to Veracode's SecurityInsights service for all provisioned platform users. Third-Party SecurityReview is available at varying subscription levels or may be purchased a la carte per vendor application.