

Veracode Vendor SecurityReview®

Highlights

Enterprises use Vendor SecurityReview To:

- Establish Secure Procurement Initiatives
- Shift the responsibility and cost of application security back to vendors
- Evaluate vendors as part of the RFP process
- Set minimum security thresholds for purchased software
- Understand risks in mergers & acquisitions

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
- **No Source Code Required** – The source code of COTS software is rarely available for testing. For the first time, organizations can test commercial software by using Veracode’s patented binary analysis

The burden of minimizing risk and controlling operational cost from insecure third-party software has been placed largely on the enterprises purchasing commercial off-the-shelf (COTS) applications. In most cases corporations do not have any insight into what vulnerabilities exist in these applications, resulting in an unacceptable level of unbounded risk. Veracode’s on-demand Vendor SecurityReview allows organizations to qualify and quantify the risk found across their extended supply chain in a simple and cost-effective manner.

Enterprises and the State of COTS Security

Enterprises face an uphill battle in controlling security risks across their extended software supply chain. The increased importance of third-party software and service providers, the interconnectivity of software systems as well as the proliferation of Web services and SOA have coincided with hackers moving up the IT stack to use applications as the front door to gain access to corporate assets. In fact, analyst firm Gartner has reported that 75% of new attacks are targeted directly at the application layer while software vulnerabilities have reached an all time high with over 7,000 new vulnerabilities disclosed over the past year according to the National Vulnerability Database.

At the same time, quantifying the risk associated with purchased software has been difficult to date. Testing such applications before deployment has been nearly impossible due to the lack of access to source code (intellectual property). Automated black box tests using dynamic scanning tools are restricted to Web applications only and do not help with looking at back-office components and n-tier applications. Manual penetration tests are time consuming, costly and hit the budgets of enterprises trying to do the right thing. As a result, enterprises either do not test COTS applications at all or are restricted to analyzing a small sub-set of their purchased software which results in unbounded risks to the organization.

Secure Procurement Governance

The best defense and easiest way to reduce security risks is to not let those very risks enter the organization from the outset. Efforts to ensure software is secure as part of the procurement process have focused on demanding the vendor to show a certain level of application security competency or to attempt to include liability clauses as part of the contract process. However, many contracts that originate from the vendor are written to protect the vendor and not the enterprise purchasing software. CISOs and VPs of Procurement need to move to a proper procurement governance model that builds security assessments directly into the procurement process.



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

Joseph Feiman
VP & Gartner Fellow

Enterprise Benefits

- Shift the responsibility and operational cost of application security from their organization back to providers
- Minimize unbounded risk associated with third-party software and service providers
- Establish mitigating controls by creating thresholds for purchased software, before it is deployed in-house
- Develop a security procurement governance model that delivers permanent and persistent success for the business through excellence in procurement.

Vendor Benefits

- Obtain detailed insight into the security risk of commercial software products market offerings
- Proactively execute actionable remediation roadmap
- Leverage Veracode's ratings to differentiate and market security as a key feature and selling point from competitive offerings



Secure Procurement Initiative

Veracode has developed the Secure Procurement Initiative to meet this need and enable organizations to create and implement compensating controls for security risk. Sponsored by Veracode who provides the industry's first standards-based security rating, the goal of the initiative is to create demand for secure software which will influence software suppliers to embed security into their products.

Key objectives of the Secure Procurement Initiative:

- Increase awareness of secure application development capabilities and specific application risk among the independent software vendor (ISV) and service provider community
- Create a consistent, objective application security risk framework based on well-known industry-standards
- Reduce time, effort and cost incurred by enterprises in conducting security assessments
- Provide baseline assessments to allow enterprises to focus on risk mitigation strategies for gap areas with IT vendors
- Assist independent software vendors to easily and cost-effectively fix security vulnerabilities to satisfy the demand for secure software.

Veracode Vendor SecurityReview®

Veracode Vendor SecurityReview is the industry's first automated, on-demand application security assessment solution specifically designed to help enterprises and government agencies quantify and manage security risks of third-party applications.

Veracode's Secure Procurement Initiative is based on two key technology breakthroughs:

1. automated security assessments conducted against binary code (executables); and
2. an on-demand platform that integrates multiple application security testing techniques capable of servicing the global software supply chain

Standards-based Independent Assessment

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 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.

For More Information

For information on software security services, best practices, and methodologies, contact us at.

Veracode, Inc.
 4 Van de Graaff Drive
 Burlington, MA 01803
 Phone: +1.781.425.6040
 Email: contact@veracode.com
www.veracode.com

SecurityReview is a registered trademark of Veracode, Inc.