

# Veracode COTS SecurityReview®

## Highlights

### Enterprises use COTS 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 organizations do not have any insight into what vulnerabilities exist in these applications, resulting in an unacceptable level of unbounded risk. Veracode’s on-demand COTS SecurityReview helps enterprises and government agencies quantify and manage security risks of commercial off-the-shelf software before it is deployed in-house.

### 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.

### Automate Vendor Security Audits & Acceptance Testing

Veracode enables enterprises to conduct vendor security audits by a trusted entity on the final application code as part of an organization’s formal software acceptance process, without the need for source code or costly on-site consultants. Veracode inspects the application at the same level that it is attacked – the binaries. By assessing the final application code, Veracode ensures that all threats, including vulnerabilities and malicious code are detected, thereby providing the most complete security audit across your extended supply chain. Additionally, Veracode delivers its offerings as a software-as-a-service (SaaS), ensuring that applications can be independently verified and validated, irrespective of their source without costly investments in hardware, software or training.



“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



## Working Collaboratively with Vendors

Veracode COTS SecurityReview helps enterprises and their software suppliers deal with the difficult task of scanning code and establishing security guidelines for the extended software supply chain. Since enterprises typically cannot or do not want to take on potential liability issues of analyzing and reviewing third-party source code, Veracode provides the ideal solution as the world's only vendor that can inspect software executables (binary code) without asking vendor to expose any of their intellectual property in the form of source code. Without changing any of the enterprises' or vendors' internal processes, Veracode delivers a fully automated analysis within 24 to 72 hours and assigns a security rating for each application.

## Standards-Based Independent Verification & Validation

As an independent and trusted provider of automated security ratings, Veracode conducts 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 based on a standards-based scoring system, leveraging MITRE's Common Weakness Enumeration (CWE) for classification of software weaknesses, 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 and vendors use to set security thresholds and embed into acceptance criteria.

## Protect Your Enterprise from Backdoors in Commercial Applications

As software development has grown more complex, it has become a multi-tier process with many parties involved. Commercial applications are now comprised of code developed by the vendor, open source, sub-contractors, offshore providers and third party components which has resulted in new types of threats – such as those coming from backdoors which can allow remote access to hackers – and are impossible to spot with traditional tools. Research from the US Department of Homeland Security points to a significant risk from backdoors and 23% of software packages used by US government employees have backdoors built into them. Only Veracode's COTS SecurityReview is specifically designed to detect backdoors in commercial software through our patented binary analysis technology and protect enterprises from this critical threat.

## 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)