

## Key Facts

### Independent, Trusted Reviews

#### Separation of Duties

- Consistent, repeatable assessments using industry standards CWE and CVSS
- Independent customer or regulatory documentation
- Ensures oversight and audit trail

#### Regulatory Compliance

- Turnkey Security Best Practices Solution
- Supports key control processes for PCI, FISMA, GLBA, HIPAA and other regulations

*“Businesses should urge all IT vendors to use CVSS in their vulnerability and patch reporting.”*

John Pescatore

Gartner

## Veracode's Security Ratings System

Veracode offers the industry's first standards-based rating of security levels in software. Veracode's Software Security Ratings System provide a pragmatic and repeatable method for organizations developing or procuring software to measure, compare and reduce risks related to application security.

Veracode's Ratings System is used to assess the severity and exploitability of software flaws. By producing a software security rating, enterprises now can gain insight into the security quality of software similar to that provided by Moody's®, Standard and Poor's® or Consumer Reports® for other products.

Veracode's Security Ratings System provides key benefits to both enterprises and software developers. Veracode helps organizations determine what level of risk is acceptable and acts as a trusted broker. Veracode takes great care to ensure enterprises have insight to the applications they deploy while simultaneously respecting the vendors' right to privacy and subscribing to responsible disclosure principles. All detailed vulnerability information is provided solely to the owner of the intellectual property along with a "remediation roadmap" for quickly improving the security and rating for the applications.

### Based on Industry Standards

Veracode's Software Security Ratings System is based on respected industry standards including 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. Veracode is the only organization to combine these standards into a meaningful and practical way to assess software security across internally developed and externally purchased applications.

Veracode was the first application security vendor to implement CWE as a standard identifier and it is now becoming broadly adopted across the application security space by many other vendors and security practitioners. Each identified flaw is associated with a CWE ID and a severity weight based on the confidentiality, integrity, and availability impacts for that flaw as defined by the Common Vulnerability Scoring System (CVSS).

CVSS is utilized by the National Vulnerability Database and by major software companies such as Cisco and Oracle to prioritize their security remediation and establish compliance initiatives such as PCI. Additionally Gartner has stated that CVSS should be incorporated by IT vendors for vulnerability and patch reporting. The severities of all security flaws are aggregated and normalized to a scale of 0 to 100, where 100 is a perfect score. The score generated by a particular type of testing (automated static, automated dynamic, or manual) and the application's assurance requirements are then used to compute the application's rating for each testing methodology.

*“The industry needs a way to measure how secure software is, whether that software is purchased, built in house or comes from an outsourced developer. The ability to rate software security levels allows companies to manage risk by determining whether or not the software meets their requirements.”*

*Diana Kelley, Analyst*



## The Power of Additive Analysis Techniques

To achieve the industry's most complete security assessment, Veracode applies multiple automated testing analyses including white box testing (static binary analysis), black box testing (dynamic Web application analysis), and for the most the mission-critical applications manual penetration testing. This helps accommodate the complexity of Web 2.0 and consumer-like web applications that enterprises are increasingly using.



## What do the Ratings mean?

The Veracode Rating System provides practical insight into the current security of internally or externally developed software and a remediation roadmap to improve the overall security posture of software. The ratings, which are offered in a three-letter system, are based on multiple software security testing techniques. The assurance level of the software determines whether one, two or all three testing techniques are used.

The first letter in a software rating represents automated static binary analysis testing, the second letter represents automated dynamic analysis testing and the third letter represents human testing. The letters run from "A" to "F", skipping "E." Veracode believes high assurance applications require all three testing techniques and has built the ratings service and service platform to incorporate and integrate all three.



## 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  
Tel: +1.781.425.6040  
Fax: +1.781.425.6039  
URL: <http://www.veracode.com>

Veracode and Veracode SecurityReview are trademarks or registered trademark of Veracode, Inc.