

Veracode's Ratings System in Brief

What is an application security rating?

Veracode's Ratings provide an independent assessment of the security level of applications developed in-house or purchased from a third-party. The rating quantifies the security risk based on types, number and severity levels of security flaws identified in the application. The rating (grade) is generated based on automated static binary, automated dynamic and/or manual security analysis techniques.

How do enterprises use software ratings?

Enterprises use Veracode's ratings to reduce the levels of unbounded risk associated with the procurement of insecure software. Through the ratings, enterprises establish security thresholds for commercial off-the-shelf (COTS) applications before they enter their organization, thereby greatly reducing the operational risk and capital requirements for their companies without compromising the intellectual property of software vendors. The ratings create transparency for the security of third-party applications, help establish compensating controls and embed security best practices into the procurement process.

What types of applications does Veracode rate?

Veracode is the only vendor assessment that can rate any third-party software or internally developed application regardless if the application is stand-alone, multi-tiered or part of an interconnected system without requiring any source code. Veracode assesses 100% of the application code including third-party libraries for any application written in C/C++ on Solaris, Windows and Linux, as well as any Java application on any platform as well as scripting languages. We will support C# and .NET applications shortly.

What types of security risk does Veracode rate?

Based on its patented binary code analysis and the combination of multiple testing techniques, Veracode analyzes the key application security risks that matter most to enterprises including the most prevalent vulnerabilities, the absence and presence of security features (e.g. encryption) and backdoors in third-party code (e.g. hardcoded passwords) that may lead to insider fraud and cyber terrorism. Veracode provides a more complete assessment compared to conventional tools based on its on-demand service and the combination of multiple testing techniques integrated into a single user experience.

What types of flaws does Veracode identify?

Veracode's ability to find the most critical security flaws is based on the industry-standard Common Weakness Enumeration (CWE) and also draws from additional sources such as security analysis from National Institute of Standards and Technology (NIST) and the Open Web Application Security Project (OWASP) Top Ten 2007. Based on these sources and the findings of its research team, Veracode has assembled a list of the top application security flaws which provides

the greatest threat to enterprises. These include cross-site scripting, SQL injection, PHP include, buffer overflow, directory traversal, info leak, integer overflow, bad permissions, format string, bad privilege assignment, symbolic link, untrusted search path, CRLF injection, memory leak and other vulnerabilities.

What is Veracode's rating process?

First, an assurance level is assigned for each application based on business risk factors such as: reputation damage, financial loss, operational risk, sensitive information disclosure, personal safety, and legal violations. Up to three assessment techniques are then conducted based on the assigned assurance levels. The most business critical applications (highest assurance level) will undergo automated static binary analysis, automated dynamic analysis and manual penetration testing.

What do Veracode's ratings mean?

The basis for Veracode's rating is the Security Quality Score (SQS). 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 each type of assessment (automated static, automated dynamic, or manual) is then mapped to a rating given the application's business criticality (assurance requirements). Higher assurance applications require a higher score than lower assurance applications to receive an A rating. Since Veracode assigns a rating to each application that is assessed, enterprises gain insight into the security quality of software they have purchased similar to that provided by Moody's®, Standard and Poor's® or Consumer Reports® for other products. The best possible score an application can achieve is AAA.

What sources of information does Veracode use?

Veracode analyzes 100 % of the application including any third-party linked libraries. Veracode's Ratings are based on 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. According to Gartner "CVSS represents the best available standard for repeatable and referenceable vulnerability risk ranking," and " CVSS support should be a requirement for all vulnerability assessment procurements and enterprises should urge all IT suppliers to use CVSS scoring when disclosing vulnerabilities."

What does the "Verified by Veracode" logo program stand for?

The "Verified by Veracode" logo is a quality seal for software applications that highlights a minimum level of security for applications that have achieved at least an "A" rating or better for a particular testing technique.