

VerAfied™ Security Mark in Brief

What is the VerAfied™ security mark?

The VerAfied security mark is quality indicator for the security level of applications and software components. Veracode's ratings are completely transparent and based on industry accepted standards for software assessment from NIST, CWE and CVSS against vulnerability benchmarks such as the OWASP Top 10 and CWE-SANS Top 25.

How do enterprises use the VerAfied™ security mark?

Enterprises use security 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 VerAfied security mark creates transparency for the security of third-party applications, help establish compensating controls and embed security best practices into the procurement process.

How do ISVs use the VerAfied™ security mark?

ISVs use the VerAfied security mark to demonstrate that their software has been rigorously assessed against industry standards and enables the provider to market the security of their software as a competitive differentiator. The security assessment also lowers their operational costs by building higher security quality applications requiring fewer patches or maintenance.

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++, Java, C#.NET, ASP.NET, VB.NET, and Windows Mobile across common Solaris, Windows and Linux platforms.

What types of security risk does Veracode rate?

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 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 CWE-SANS Top 25 Most Dangerous Programming Errors and the Open Web Application Security Project (OWASP) Top Ten. These include cross-site scripting, SQL injection, , buffer overflow, directory traversal, info leak, integer overflow, and other critical vulnerabilities.

What is the VerAfied 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 does the VerAfied security mark mean?

The VerAfied mark signifies that an application has received an independent application risk management assessment from Veracode and the provider has resolved or mitigated any vulnerabilities identified. Due to the nature of software security testing, no organization can guarantee that the lack of discoverable flaws means their software is completely secure. However, through rigorous independent testing using Veracode's automated static binary analysis, automated dynamic web vulnerability scanning, enhanced dynamic analysis testing, and/or manual penetration analysis these organizations have utilized the most widely accepted and comprehensive methods available to secure their software.

What sources of information does Veracode use?

Veracode analyzes 100 % of the application including any third-party linked libraries. The VerAfied security mark is 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."