VERACODE | FACT SHEET

HIGHLIGHTS

- ✔ Veracode delivers the first comprehensive application security testing program to enterprises looking to quantify the risk posed by purchased applications.
- ✔ VAST programs enable enterprises to make informed decisions about the risk associated with software sourced from independent software suppliers.
- ✔ Veracode's patented binary static analysis and dynamic analysis technology scan third-party software without the need for source code, as recommended by the Financial Services Information Sharing and Analysis Center (FS-ISAC).
- ✔ Veracode acts as an independent third party, offering trust and mutual assurance to both the enterprises requesting security testing and the software suppliers providing software for testing.
- ✔ Veracode protects the software vendor's intellectual property rights while verifying security posture. We provide detailed, prioritized remediation guidance to help software vendors fix critical security flaws.

Veracode VAST Program

The Veracode Vendor Application Security Testing (VAST) program helps enterprises to understand and reduce the security risks associated with vendor-supplied software.

The typical enterprise software ecosystem has become big, complex and insecure, often due to the increased reliance on externally developed applications. Every company needs to manage the risks inherent in its reliance on vendor-supplied software to run the business. Unfortunately, most IT organizations do not have the time, budget or internal resources to run a meaningful vendor application security compliance program.

Traditional assessment methods are often either expensive and unscalable, or minimally invasive and non-representative of the security of the software products.

In addition, software vendors are reluctant to share access to their proprietary software code for security assessments. The result: Most enterprises carry too much risk across their software portfolio.

Managing Risk in the Software Supply Chain

All enterprises assume some risk in using software sourced from vendors and suppliers. However, most enterprises assume unnecessary and unmitigated risk by accepting insecure vendor applications in their software supply chain. Insecure vendor software is subject to exploitation by hackers and criminals, which puts the entire enterprise at risk of loss of data, revenue and reputation.

At the same time, in order to speed innovation, enterprises are increasing their reliance on third-party software, with over two-thirds of the average enterprise's application portfolio sourced from third parties – either commercial software vendors or developed by an outsourcer (source: IDG study, "Majority of Internally Developed Apps not Assessed for Critical Security Vulnerabilities" June 2014). Yet the typical enterprise's portfolio of third-party software carries unquantified risk. In one case, a global industrial manufacturer found that more than 90 percent of the third-party software it tested had significant, compromising flaws (source: Veracode case study, "Global Industrial Manufacturer Secures its Software Supply Chain").

To manage this problem, existing governance, risk and compliance efforts must extend to vendor risk management practices. Regulations such as SOX, MAS and PAS 754 mandate that privacy and security controls extend to a company's software vendors and solution providers. Further, recommendations by bodies such as the FS-ISAC and NIST include security testing of third-party software in their best practices for enterprise security.

Enterprises must analyze and attest the security posture of all vendor-supplied applications in their portfolio to speed audit compliance and meet policy requirements. However, internal IT vendor management and security teams are so often overwhelmed by the scope of this problem.

To succeed, enterprises must pursue a systematic course of action that partners with — not punishes — vendors. Veracode provides testing capabilities to enterprises through the VAST program. The program provides trust and mutual assurance to both the enterprise customer and its software suppliers regarding the security of the company's vendor-sourced software portfolio.

VERACODE

FACT SHEET

Veracode's Vendor Application Security Testing capabilities combine our testing technologies with program management and vendor engagement to address third-party software risk.

DAST: Quantify risk from third-party web applications and identify vulnerabilities in running web applications, before they are exploited.

Veracode's dynamic testing capabilities are leveraged on your perimeter and behind the firewall in your QA environment to ensure that the software you are purchasing, installing and distributing to your enterprise meets your security requirements.

With Veracode's DAST, you will:

- Understand if customizations made to the web app introduce new risk.
- Test without requiring source code from your vendors.
- Determine if additional testing and remediation efforts are necessary.
- Understand your risk before deploying new applications.
- Test during your procurement process.

SAST: Analyze all third-party applications with Veracode's patented binary static analysis technology, which does not require source code for security testing.

Veracode's binary SAST analyzes binary code to create a detailed model of the application's data and control paths. The model is then searched for all paths through the application that represent a potential weakness. A report of these weaknesses or vulnerabilities is supplied to the developer of the software so that it can address the issues in order to meet your security requirements.

With Veracode's SAST, you will:

- Understand the security posture of all your third-party applications.
- Engage your software producers to address security findings for improved security of your applications.
- Understand your risk before purchasing new applications.
- Test during your procurement process.
- Address regulatory requirements and best practices such as MAS, FS-ISAC and PCI 3.0.

Program Management and Outreach: Scale your vendor application security testing initiative by leveraging Veracode for program management and engagement with your software suppliers.

Veracode combines application security expertise, proven processes and cloud-based testing technology to augment your vendor application security testing program. By leveraging Veracode for program management and vendor outreach, enterprises gain a systematic method for engaging and testing vendor-produced software at a large scale and with the goal of ultimately embedding security into the development process for all the software you are purchasing.

With Veracode's Program Management and Outreach, you will:

- Ensure security testing requirements are understood by your software vendors.
- Provide your vendors with a systematic, standardized method to respond to your security testing needs.
- Scale your security testing program across your application portfolio.
- Benchmark your vendor application security testing program against your peers within and across industries.

Veracode's cloud-based service and systematic approach deliver a simpler and more scalable solution for reducing global application-layer risk across web, mobile and third-party applications. Recognized as a Gartner Magic Quadrant Leader since 2010, Veracode secures hundreds of the world's largest global enterprises, including 3 of the top 4 banks in the Fortune 100 and 20+ of the world's top 100 brands.

VERACODE
The Most Powerful Application Security Platform on the Planet