VERACODE

IMPERVA PARTNERSHIP

Highlights

- Simplify compliance with PCI DSS requirement 6.6 which recommends implementation of both DAST and WAF technologies to build a multi-layered defense against web attacks.
- The use of both DAST and WAF technologies together allows organizations to better prioritize their remediation efforts based on suspicious attack patterns observed by the WAF.
- Imperva SecureSphere WAF combines multiple defenses together to stop automated attacks.
- SecureSphere provides the most flexible deployment options of any WAF in the industry, including a unique drop-in deployment that requires no changes to existing applications or network.
- Veracode's DynamicDS solution inspects applications at run-time, the same way a hacker would attack them, providing accurate and actionable vulnerability detection.
- Veracode DynamicDS automatically removes false positives from its results reporting so teams don't waste time on erroneously flagged issues.
- Veracode DynamicDS can be scaled quickly to test multiple applications in parallel.

Veracode and Imperva Partner to Secure Websites

Veracode and Imperva have partnered to integrate Veracode's DynamicDS, a dynamic application security testing (DAST) service, into Imperva SecureSphere, the industry leading web application firewall (WAF) solution. The integrated solution will enable security teams to maintain a high level of protection on websites.

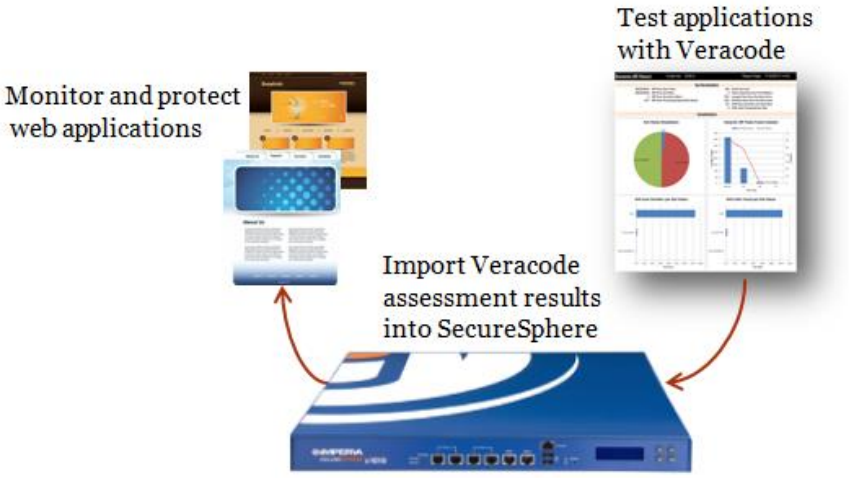
Why integrate DAST and WAF technologies?

When a security incident occurs, time is not on your side. A website can be hijacked or breached before there is time to fix the web application vulnerability that caused it. In some cases, the original source code or skilled development expertise simply aren't available to put in a timely fix. It takes too long to configure WAFs with custom patches that effectively block all known vulnerabilities, not to mention new and emerging threats.

How the Veracode/Imperva Integration Works

Veracode's DynamicDS service links directly to Imperva SecureSphere to provide specific protection from known attacks. Veracode uncovers software vulnerabilities in critical applications and Imperva helps to shield those applications from exploits on any specific flaws identified. Organizations can create custom rules to apply application security policies for rapid threat response and risk mitigation.

Veracode's DynamicDS service produces dynamic scan results that are converted to a format that Imperva SecureSphere can read, so the WAF can process more specific information on how to prevent security breaches. Powering a WAF with this detailed threat intelligence is critical to protecting your critical applications against web attacks.



Veracode's web application security solution analyzes websites for security flaws and then the Imperva SecureSphere WAF virtually patches discovered vulnerabilities.

Benefits to the Enterprise

- **Reduced application risk**. Respond quicker with more accurate detection and swifter prevention measures until flaws in code can be fixed.
- **Reduced operational cost**. Why pay high cost consultants to build custom rules? Why waste security and development time chasing false positive results?
- **Increased uptime**. Manually implement and maintain vulnerability code repairs at scale while maintaining application uptime and performance.
- **Easier compliance.** Meet industry and regulatory mandates such as PCI-DSS 6.6 that specifically recommend both DAST solution and WAF as part of a layered security stack. This is integration made effortless.

Benefits to Security Teams

- **Faster response to security incidents**. CISOs and security teams can demonstrate faster incident response times to security threats before exploits result in a data breach, narrowing the window of exposure while buying developers valuable time and flexibility.
- **Increased protection due to closed loop security intelligence**. The knowledge sharing provided by this DAST-WAF integration enables a new type of closed-loop security intelligence that empowers security teams to better protect organizations from web application exploits.
- **No false positives**. False positives are a common side effect of on-premise scanning tools and poorly executed DynamicDS/WAF integrations. Irrelevant findings lead to an excessive amount of blocking rules, which slow performance and effectiveness. Veracode DynamicDS automatically removes false positives from its results reporting so teams don't waste time on erroneously flagged issues.
- **Increased accuracy**. Generic rules amount to a "one size fits all" approach that can't possibly cover all use cases, are easily circumvented by hackers and sometimes block good traffic. Applying custom WAF rule sets provides better protection against known malicious threats.
- **Ease of use**. After every scan, rules can be downloaded instantly, with easy step-by-step instruction on how to upload from Veracode to Imperva.

About Veracode

Veracode DynamicDS is a DAST service that provides fully automated web application vulnerability scanning. DynamicDS empowers any organization to identify and remediate security issues in their running web applications before hackers can exploit them. DAST solutions like DynamicDS test the live-running version of the application – whether in QA, Production, or behind-the-firewall.

The cloud based Veracode platform combines patented static, dynamic and manual testing, extensive eLearning capabilities, and advanced application analytics to help enterprises develop scalable, policy-driven application risk management programs. Veracode delivers unbiased proof of application security to stakeholders across the software supply chain while supporting independent audit and compliance requirements for all applications no matter how they are deployed, via the web, mobile or in the cloud.

About Imperva SecureSphere

The Imperva SecureSphere Web Application Firewall (WAF) protects applications from current and future security threats by combining multiple security engines into a cohesive Web defense. Certified by ICSA Labs, SecureSphere provides ironclad protection against the OWASP Top Ten, including SQL Injection, XSS and CSRF, and it addresses PCI DSS requirement 6.6

The SecureSphere WAF offers organizations drop-in deployment, automated, adaptable security, and low operational overhead, providing your business with a practical and highly secure solution that ensures your Web applications and data are safe. As the market-leading Web Application Firewall, more organizations rely on Imperva to monitor and protect their critical Web applications than any other vendor.

Imperva Inc.
3400 Bridge Parkway, Suite 200
Redwood Shores, CA 94065

Tel +1.650.345.9000
Fax +1.650.345.9004

www.imperva.com

Veracode, Inc.
65 Network Drive
Burlington, MA 01803

Tel +1.339.674.2500
Fax+1.339.674.2502

www.veracode.com