VERACODE | FACT SHEET

HIGHLIGHTS

- ✔ Performs a deep scan of all critical internal and external web applications at run-time.
- ✔ Provides deep visibility into web application risk and vulnerabilities before cyber-attackers can exploit them.
- ✔ Backed by world-class security experts who verify/prioritize results.
- ✔ Also assesses web applications behind the firewall using a virtual appliance.
- ✔ Integrates dynamic scan results into existing WAFs to rapidly mitigate risk.
- ✔ Automates compliance reporting for PCI, HIPAA, SOX, NIST, MAS and other regulatory mandates.
- ✔ Delivered via unified cloud-based platform for securing web, mobile, third-party and open source applications.

DynamicDS (DeepScan)

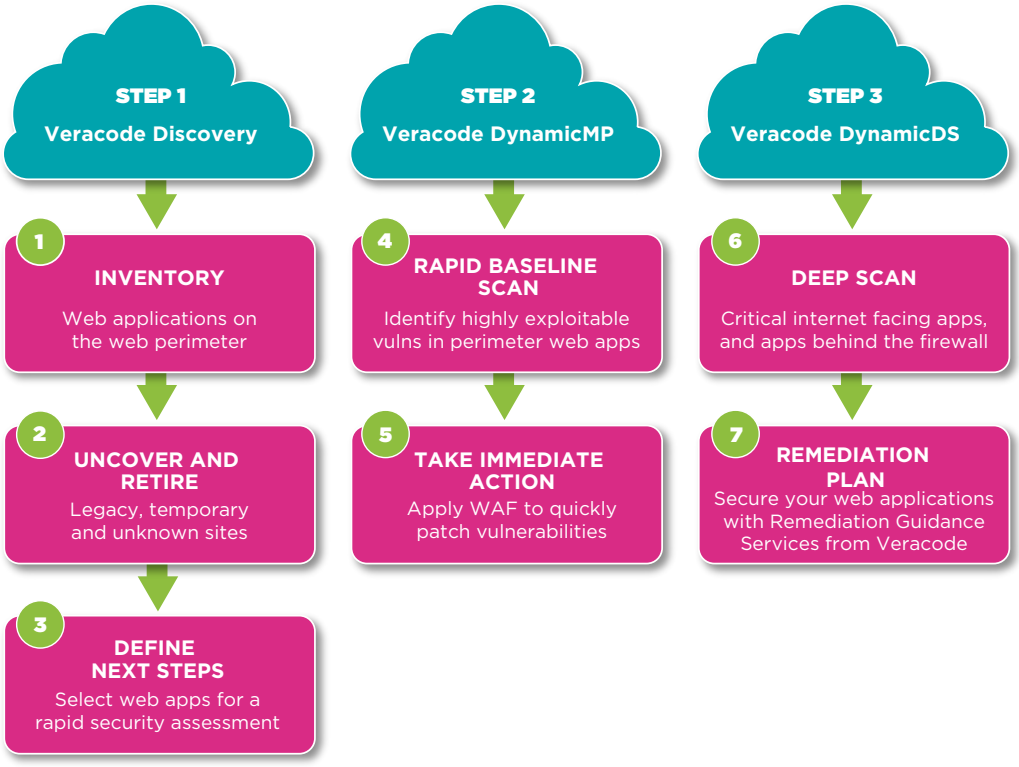
Secure your web application infrastructure — at scale — with our automated cloud-based service.

With all businesses becoming digital businesses, enterprises are increasingly concerned with reducing risk from the expanded web perimeter created by the sum total of all their web applications — whether developed internally, using outsourcers or procured from third-parties such as SaaS vendors.

Most organizations lack the in-house resources and expertise to continuously assess the security of this vast global attack surface. Further complicating this effort, your attack surface is constantly changing as new websites are launched on an almost daily basis by business units throughout your organization. What if you could continuously scan all of your web applications the same way a cyber-attacker would — except at massive scale?

DynamicDS (DeepScan) is a Dynamic Application Security Testing (DAST) technology that provides granular visibility into the risk posture of all your web applications, with fewer in-house resources. It identifies application vulnerabilities before cyber-criminals can find and exploit them. DynamicDS delivers ongoing security assessments as an automated cloud-based service — backed by Veracode's world-class application security experts.

3 Steps to Web Application Security



VERACODE

FACT SHEET

BENEFITS

- ✓ Simplest, fastest way to automate assessments without requiring additional resources.
- ✓ Reduces enterprise-wide risk via centralized policies, metrics and reporting.
- ✓ Centralizes best practices across disparate business units and development teams, including outsourcers and SaaS providers.
- ✓ Simplifies information sharing and audit/approval workflows across all key stakeholders via role-based access control (RBAC).

First-generation, on premises scanning tools are complex and require in-house experts or expensive consultants to configure them and interpret their results. Plus they don't provide the same level of flexibility and massive scalability as an auto-scaling cloud service. DynamicDS combines the power of automated, policy-based security with verified results, all on a centralized cloud-based platform.

DynamicDS works in conjunction with Veracode's Web Application Perimeter Monitoring (Web APM) solution. Step 1 starts with Discovery and proceeds to Step 2 where DynamicMP performs lightweight unauthenticated scans of all your web applications. This quickly identifies easily-exploitable vulnerabilities such as SQL injection and Cross-Site Scripting. Web APM uses a massively parallel, auto-scaling cloud infrastructure to rapidly baseline your risk — across tens of thousands of domains — in days versus weeks or months.

Finally DynamicDS (Step 3) provides deep scanning using both authenticated and non-authenticated access methods to enable continuous, ongoing monitoring of your web applications. DynamicDS leverages baseline results from DynamicMP to understand where to focus its deep scan assessments.

How It Works

DynamicDS performs a comprehensive "black-box" scan from the outside-in to identify critical web application vulnerabilities using both authenticated and non-authenticated access. It looks for threat vectors that are easy to find and exploit from the OWASP Top 10 and the CWE/SANS Top 25 including SQL Injection, cross-site scripting (XSS), insufficiently protected credentials, configuration errors and information leakage. It probes the attack surface using the same techniques as a cyber-criminal, such as deliberately supplying malicious data to input fields of web forms and shopping carts. Legacy scanners identify only simple signature-based attacks without examining the structure of the underlying application, resulting in poor coverage and inaccurate results.

Key Capabilities

Web 2.0 Ajax support: Supports all server-side technologies including Java, J2EE, ASP, ASP.NET, Ruby on Rails, JavaScript, Perl and Python as well as client-side components in JavaScript or Flash.

Intelligent crawling: Understands the entire attack surface to determine vulnerability attack vectors — much like an attacker would.

Deep platform understanding: Delivers accurate and actionable results using its knowledge of language — and platform-specific weaknesses to test probable attack methods.

Multiple authentication methods: Supports browser-based and forms-based logins as well as client certificate authentication for compatibility with the widest range of applications. Specific interactions can be recorded and played back to exercise situational business logic such as shopping carts and forms.

Verified results: Dynamic scan engineers verify results to distinguish real problems from false positives.

Remediation advisory services: World-class application security experts provide detailed information on how to prioritize and fix flaws so developers don't waste valuable time.

Actionable information: Delivers complete threat information enabling development and QA teams to prioritize and remediate flaws. An industry-standard methodology measures both severity and real-world exploitability.

VERACODE

FACT SHEET

Secure web applications in production or pre-production — without additional resources

Whether your web applications are live or pre-production, DynamicDS gives you a highly-automated approach to easily scale your application security program. It's easy to deploy, easy to use. Scan hundreds of applications without straining IT operations resources or relying on manual penetration testers to perform repetitive tasks that can easily be automated.

Then Veracode's remediation advisory service, provided by world-class security experts, helps you rapidly prioritize and mitigate the most critical vulnerabilities first and demonstrate return on investment fast. Our DynamicDS engineers also verify results to ensure consistent, highly accurate findings — saving time and effort.

DynamicDS can also integrate its security intelligence with your existing Web Application Firewall (WAF) to enable rapid mitigation of critical vulnerabilities. This "virtual patching" approach enables WAFs to have the latest information on specific application threats so they can better shield applications from exploits in real-time. Combining Veracode DAST results with your WAF makes its protection more effective, protecting your investment.

VIRTUAL APPLIANCE FOR SCANNING APPLICATIONS BEHIND THE FIREWALL

To secure web applications behind the firewall, Veracode's Virtual Scan Appliance (VSA) is a pre-configured virtual appliance that implements the DynamicDS engine. With no hardware to purchase or software to configure, it's easy to deploy in an unlimited number of data centers to scale across your entire web application infrastructure.

The VSA is used to perform detailed dynamic security assessments during pre-production/QA — before application deployment. It also protects critical internal applications from insider attacks or attacks by malicious outsiders who gain access with stolen credentials. All results are consolidated with other security information through our centralized cloud-based platform.

SECURITY OF THE VSA

The VSA was carefully designed and reviewed by Veracode's security research team to protect your environment and the vulnerability information it collects.

All VSA communication originates from the VSA so there's no need to open any inbound firewall ports.

The VSA has been hardened in multiple ways — including having an encrypted file system, custom locked down shell, removal of non-essential services and no open ports other than those explicitly needed.

All data transferred to and from the VSA is encrypted when in motion and when at rest in the Veracode infrastructure. All customer flaw information on the VSA is stored in memory unless there is a service interruption, in which case it is temporarily stored and encrypted on disk.

Programmatic, policy-based approach to systematically reduce enterprise risk

Veracode helps your organization systematically reduce risk by transforming de-centralized ad-hoc processes into structured governance programs — based on best practices learned by working with some of the largest and most complex organizations in the world.

This programmatic approach is enabled by:

- **An end-to-end cloud-based service** for web, mobile, third-party and open source applications.
- **A unified cloud-based platform** for multiple assessment techniques including SAST, DAST, Software Composition Analysis for cataloging vulnerable third-party and open source components, behavioral analysis of mobile applications, and manual penetration testing.
- **Centralized policies, metrics and reports** to systematically reduce risk and measure progress in a consistent manner across disparate business units and development teams, including outsourcers.
- **World-class security experts** that help enterprises rapidly mitigate and remediate vulnerabilities — not simply identify them — via on-demand remediation advisory services and ongoing training.

To learn more, see: www.veracode.com/products

Veracode's cloud-based service and programmatic, policy-based approach deliver a simpler and more scalable solution for reducing global application-layer risk across web, mobileand 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 25+ of the world's top 100 brands.

VERACODE
The Most Powerful Application Security Platform on the Planet