VERACODE | FACT SHEET

Web Application Perimeter Monitoring

Discover and protect all of your web applications in a fast and scalable way.

Many enterprises don't know how many public-facing websites they own, such as external cloud-hosted sites, sites acquired via mergers and acquisitions and temporary sites created by outside agencies and contractors in multiple business units worldwide.

Our massively parallel, auto-scaling cloud infrastructure uses advanced search techniques to rapidly discover all public-facing applications and lightweight dynamic analysis to quickly identify the most exploitable vulnerabilities — such as SQL Injection and Cross-Site Scripting (XSS).

Web application perimeters are constantly expanding as organizations spin up new websites for new marketing campaigns or geographies, acquire companies and create web portals for customers and partners. Most enterprises also have legacy and old marketing sites which may be hidden or forgotten. Cyber-attackers look for the paths of least resistance — such as obscure or out-of-date websites — to gain access to critical corporate and customer data.

Our cloud-based platform enables rapid mitigation of security risk on the perimeter. Use our platform to quickly identify risk — and then take immediate action by shutting down legacy sites or feeding security intelligence about specific vulnerabilities to your existing web application firewalls (WAFs). Over time, our Web Application Perimeter Monitoring solution systematically reduces your enterprise's global application threat surface.

How It Works

Web Application Perimeter Monitoring is an end-to-end dynamic assessment solution that starts with application discovery, performs baseline scanning of thousands of applications in parallel and ends with deep scanning to enable continuous, ongoing monitoring of your web application perimeter. Veracode provides visibility into all websites in your domain including unknown sites outside your normal corporate IP range. Unlike network scanners, it uses a combination of advanced search techniques — such as DNS keyword searches, production-safe crawling, analyzing page redirects and machine learning — to quickly identify unknown sites that traditional scanners miss.

Application Perimeter Monitoring addresses web application security in three steps:

1. Discovery closes the visibility gap by creating a global inventory of all public-facing web applications. Leverage the platform's production-safe application- layer crawling and auto-scaling infrastructure to rapidly discover thousands of applications per day. Safely identify production assets such as corporate sites, sub-domains, temporary marketing sites, portals, mobile sites, international domains, acquired sites and related sites outside your domain such as "info" and "mail."

2. DynamicMP (Massively Parallel) baselines application risk by inspecting thousands of web applications simultaneously with lightweight, non-authenticated dynamic scans. It quickly

Discovery: Inventory your entire application perimeter

DynamicMP: Scan all apps quickly for critical flaws

DynamicDS: Deep scan internal and external critical apps
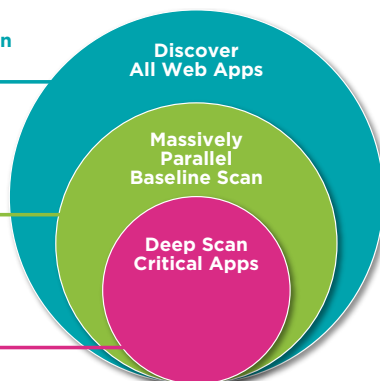
Discover All Web Apps

Massively Parallel Baseline Scan

Deep Scan Critical Apps

VERACODE

identifies highly exploitable vulnerabilities (e.g., OWASP Top 10) for rapid mitigation via WAF integration and actionable feedback for developers.

3. DynamicDS (Deep Scan) performs a comprehensive deep scan at run time to identify vulnerabilities using both authenticated and non-authenticated scans, looking for attack vectors such as insufficiently protected credentials, configuration errors and information leakage.
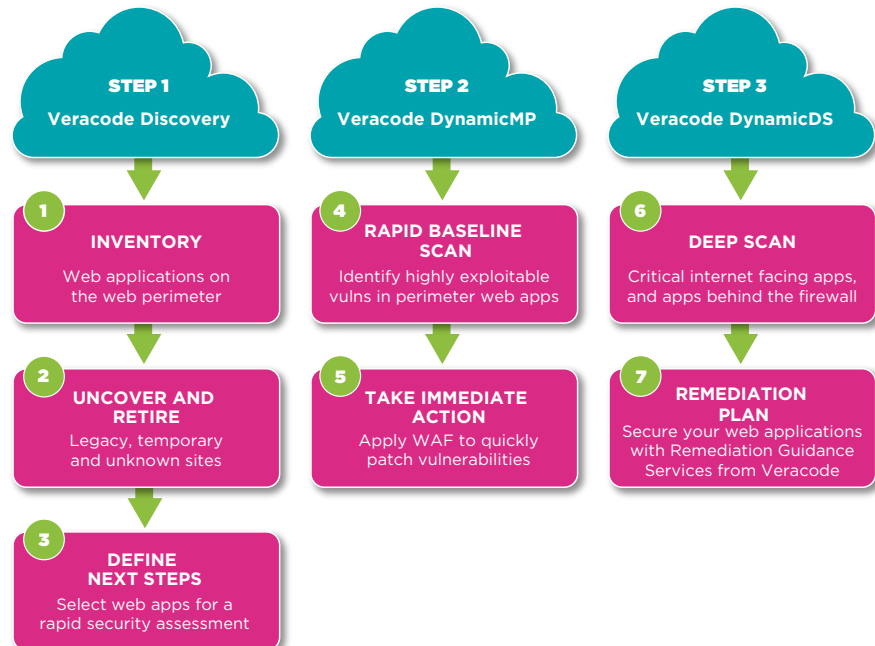
No More Blind Spots in Your Web Application Perimeter

A typical enterprise's web application threat surface grows all the time. Security teams can now replace fragmented ad hoc approaches or augment their manual penetration testing programs with an automated dynamic assessment program to protect their entire web application perimeter. Go from having blind spots across your web application infrastructure to mitigating the most exploitable vulnerabilities across thousands of apps — in days not weeks or months.

Dynamic scanning complements other assessment techniques such as static analysis (SAST), manual penetration testing and software composition analysis to find vulnerabilities in production web applications at runtime. For optimum accuracy and coverage, our cloud-based platform combines information from multiple techniques using a single set of consistent policies, metrics and reports. A centralized dashboard provides role-based access for all global stakeholders — including developers, security personnel, network operations teams and auditors — to share information and get their jobs done.

Veracode's end-to-end Web Application Perimeter Monitoring solution enables continuous, ongoing vigilance to maintain your enterprise's web security posture.

3 Steps to Web Application Security

STEP 1
Veracode Discovery

STEP 2
Veracode DynamicMP

STEP 3
Veracode DynamicDS

1 INVENTORY
Web applications on the web perimeter

4 RAPID BASELINE SCAN
Identify highly exploitable vulns in perimeter web apps

6 DEEP SCAN
Critical internet facing apps, and apps behind the firewall

2 UNCOVER AND RETIRE
Legacy, temporary and unknown sites

5 TAKE IMMEDIATE ACTION
Apply WAF to quickly patch vulnerabilities

7 REMEDIATION PLAN
Secure your web applications with Remediation Guidance Services from Veracode

3 DEFINE NEXT STEPS
Select web apps for a rapid security assessment

VERAC0DE

Key Capabilities of Web Application Perimeter Monitoring

Discovery

Load-And-Scan: Ready to go simply by providing a range of IP addresses and domain names via a web form or CSV file.

Production-Safe: Uses production-safe crawling that is no more intrusive than day-to-day network traffic.

Multiple Discovery Techniques: Includes DNS probing, light web crawling and open port checking, keywords and intelligent reasoning to understand naming conventions, page redirects, duplicates and related sites.

Application Intelligence: Provides detailed web configuration information such as protocol and port usage (e.g., HTTP vs. HTTPS), server headers (Apache, IIS, etc.), whether the site uses authentication and a site ownership confidence indicator.

Actionable Information: Generates a prioritized list of sites to quickly scan for the most exploitable vulnerabilities (e.g. SQL Injection) using DynamicMP, such as SQL Injection and Cross-Site Scripting (XSS).

Web Perimeter Inventory: Identify, scan & manage your entire web application perimeter from Veracode's cloud-based platform, whether to start a Discovery scan, view results from most recent Discovery scan or initiate DynamicMP scans.

Web Application Perimeter Monitoring systematically reduces your enterprise's global application threat surface over time.

DynamicMP

Production Safe: Scans at a very low load with negligible impact as all tests are designed and configured with production safety in mind.

Actionable Information: Delivers complete threat information, enabling development and QA teams to easily recreate and remediate flaws.

Remediation Guidance: Provides expert guidance to development teams with detailed information on how to prioritize and fix flaws uncovered.

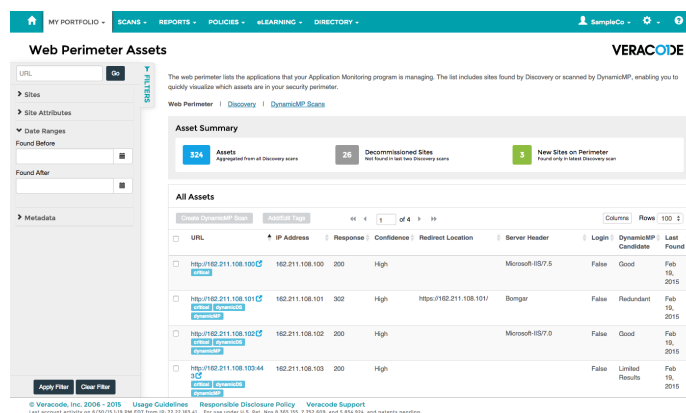**Central Policy Manager:** Ensures minimum acceptable levels of risk are uniformly applied across all applications — meeting compliance controls such as PCI, HIPAA, SOX, NIST and MAS.

Continuous Learning: Cloud-based platform continually adapts to new attack vectors and new ways in which developers use languages and frameworks.

DynamicDS

Use DynamicDS (available separately) to provide 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.

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

VERAC0DE
The Most Powerful Application Security Platform on the Planet