

# VERACODE

## VERACODE APPLICATION SECURITY

*Speed your innovations to market — without sacrificing security*

More than half of all breaches occur at the application layer, yet only 10% of enterprises test all their critical applications for resilience against cyber-attacks. Why? Because traditional application security slows down innovation.

Veracode offers a simpler and more scalable approach for reducing application-layer risk across your *entire* global software infrastructure — including web, mobile and third-party applications.

**It's Smart:** Our software learns continuously to address rapidly-evolving threats — and is designed by the world's foremost experts in application security.

**It's Cloud-Based:** Our cloud-based platform is massively scalable and let's you start immediately — without hiring more consultants or installing more servers and tools.

**It's Programmatic:** Our program managers help you implement a centralized, policy-based approach for managing enterprise-wide governance and reporting on an ongoing basis.



We help the world's largest enterprises reduce global application-layer risk across web, mobile and third-party applications.

54% of all attacks target the application layer

(Source: Verizon DBIR)

Despite this, fewer than 10% of enterprises test all of their business-critical applications before and after deploying them

(Source: SANS)

In fact, 28% of organizations don't even know how many applications they have

(Source: SANS)

# APPLICATIONS ARE STRATEGIC FOR BUSINESS INNOVATION – AND A TOP TARGET FOR CYBER-ATTACKS

79% of developers say they either have no process or an inefficient *ad-hoc* process for building security into applications

(Source: Ponemon)

87% of web applications don't comply with the OWASP Top 10

(Source: Veracode State of Software Security Report)

78% of enterprises don't perform security reviews for 3rd-party software

(Source: SANS)

## EVERY ENTERPRISE IS NOW A TECHNOLOGY COMPANY

**Mobile, cloud, social media and Big Data** are dramatically changing the way we deliver business innovation. And it's your job as CISO to ensure new applications don't introduce unnecessary risk.

The traditional, on-premises approach to application security imposes excessive complexity on fast-moving development teams. It requires specialized expertise and is difficult to configure. Plus it doesn't allow you to apply an enterprise-wide governance model with consistent policies across multiple business units and development teams.

As a result, most enterprises take a fragmented approach to application-layer security. They spend millions on *ad-hoc* manual testing and tools but cover only a fraction of their global application threat surface.

This piecemeal approach yields predictably poor results. Cyber-attackers continue to improve their tactics at an alarming rate. They look for paths of least resistance, such as less critical sites you may not even know existed. They search every nook and cranny of your applications to find their weak spots.

And if you aren't testing your application infrastructure to the same level, you're exposing yourself to unnecessary risks that can lead to theft of customer data and intellectual property, fraud, downtime and brand impact.

Veracode offers a smarter and fundamentally different approach to application-layer security. Our subscription-based service combines a powerful cloud-based platform with deep security expertise and proven best practices for managing enterprise-wide governance programs.

That's why you can count on us to make your global program successful — so your business can go further faster *without* compromising your security posture.



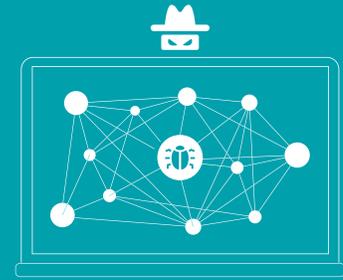
## SMART

- Continuously learning with every new scan to address rapidly evolving threats and minimize false positives
- Delivers security intelligence to existing WAFs, MDMs and GRC frameworks
- Combines multiple analysis techniques for optimum accuracy and coverage (binary SAST, DAST, behavioral analysis, manual penetration testing)
- Analytics dashboards track KPIs vs. industry peers
- Built and evolved by the world's top researchers in application-layer security



## CLOUD-BASED

- Massively scalable to address your entire application infrastructure
- Implements central policies uniformly across all business units and development teams
- Rapid ramp-up via SaaS model — no need to hire more consultants or install more servers and tools
- Centralized information-sharing platform for simplified collaboration across global teams: security, development, audit, operations, third-party vendors



## PROGRAMMATIC

- Transforms de-centralized, ad-hoc processes into structured, ongoing governance programs
- Outsourced program management leverages proven best practices developed with the world's largest enterprises
- Addresses complexity of managing across geographically-distributed development organizations
- Expert coaching helps developers rapidly remediate vulnerabilities
- Tight integration with agile workflows accelerates developer adoption
- Recognized by Gartner for receiving high marks from customers for customer success program

**BRING YOUR GLOBAL APPLICATION INFRASTRUCTURE INTO CORPORATE COMPLIANCE WITHIN WEEKS — VERSUS MONTHS OR YEARS WITH LEGACY ON-PREMISES APPROACHES**

**CISOs CAN BE MORE PROACTIVE AND STRATEGIC ABOUT APPLICATION-LAYER SECURITY — MAKING THEM BUSINESS INNOVATION ENABLERS**

# THE MOST POWERFUL APPLICATION SECURITY PLATFORM ON THE PLANET

Veracode's holistic approach combines our powerful cloud-based platform with multiple technologies and services to identify application-layer threats, including:

## Binary Static Analysis (SAST)

Static Application Security Testing (SAST), or "white-box" testing, finds common vulnerabilities by creating a detailed model of the application's data and control paths — without actually executing it.

The model is then searched for all paths through the application that represent a potential weakness, such as SQL Injection.

Unique in the industry, Veracode's patented binary SAST technology analyzes all code — including third-party software such as components and libraries — without requiring access to source code.

## Dynamic Analysis (DAST)

Dynamic Application Security Testing (DAST) or "black-box" testing, identifies architectural weaknesses and vulnerabilities in your running web applications before cyber-criminals can find and exploit them.

DAST uses the same approach used by attackers when probing the attack surface, such as deliberately supplying malicious input to web forms and shopping carts.

## Web Application Discovery & Monitoring

Most organizations have thousands of web-facing applications — including many they may not even be aware of, such as temporary marketing sites and sites inherited via M&A.

Veracode addresses this visibility gap by creating a catalog of all web applications via a massively parallel, auto-scaling cloud infrastructure that discovers tens of thousands of sites per week (via production-safe crawling).

Veracode then baselines your risk by running a non-intrusive scan on thousands of applications simultaneously. This scan quickly identifies the most exploitable vulnerabilities such as SQL Injection and Cross-Site Scripting.

Rapid mitigation is enabled by feeding threat intelligence to Web Application Firewalls (WAFs).

## Third-Party Security

More than two-thirds of enterprise applications are provided by third-parties<sup>1</sup> — including commercial applications, outsourced code, SaaS, third-party libraries and open source.

Our Vendor Application Security Testing Program (VAST) reduces the risk associated with third-party software by managing the entire vendor compliance program on your behalf and helping you define a best practices governance model.

## Mobile Application Security

Veracode's behavioral analysis dynamically analyzes an application's real-time behavior (in a sandbox) to identify risky actions such as data exfiltration to suspicious geolocations. This security intelligence is integrated with MDM solutions to enable enforcement of corporate BYOD policies.

Static analysis is also used to identify malware and coding vulnerabilities such as information leakage.

## Manual Penetration Testing Services

Manual Penetration Testing adds the benefit of specialized human expertise to our automated binary static and dynamic analysis — and it uses the same methodology cyber-criminals use to exploit specific weaknesses such as business logic vulnerabilities.

Veracode's cloud-based platform provides a single central location for consolidating results from multiple techniques — both automated and manual — so you're better able to identify all vulnerabilities of measurable risk.

## VERACODE AT A GLANCE

- Founded in 2006
- 300+ employees
- 500+ customers worldwide
- Gartner Magic Quadrant Leader for Application Security Testing

## Securing global application infrastructures for the largest and most complex enterprises including:

- One-third of the Fortune 100
- 3 of the top 4 banks
- 25+ of the top global brands

## Cloud-Based Platform

Our cloud-based platform provides centralized policies and simplifies information sharing across global teams.

It also provides: role-based access control (RBAC); security analytics and KPI dashboards to track the progress of your global program; automated compliance reporting and workflows; and APIs for tight integration with agile development processes.

## eLearning

Helps developers become proficient in secure coding practices and achieve compliance with mandates such as PCI-DSS Requirement 6.5.

1. Source: Quocirca