Veracode Application Security Testing (AST) – Leader in Gartner MQ

and

Veracode Customer Success Package

Service Definition Document

65 Network Drive, Burlington MA 01803 | +1-877-837-2203 | veracode.com

VERACODE

COMPANY INTRODUCTION

Veracode enables the secure development and deployment of the software that powers the application economy.

With its combination of automation, process and speed, Veracode becomes a seamless part of the software lifecycle, eliminating the friction that arises when security is detached from the development and deployment process. As a result, enterprises can fully realize the advantages of DevOps environments while ensuring secure code is synonymous with high quality code.

Without the need for additional staff or equipment, Veracode customers ramp up quickly, see results and prove value on day one, and consistently see improvement over time. This is due to the company's combination of,

- **Process**: Our goal is to work with your security and development teams to create an advanced program – one that reduces risk across your entire application landscape and accelerates your business. By embedding into your existing software development workflow, Veracode can ensure assessments and vulnerability remediation are completed during logical points throughout your distinct process. This seamless integration with legacy APIs has resulted in as much as 90% or greater reduction in remediation costs for our customers.
- **Platform**: The power of the Veracode Platform is in its scalability, integrations with development tools and its ability to ensure security policies are consistently enforced across the enterprise. While some companies talk about scanning 10,000 applications overall, we scanned that many applications for a single customer. Yet, the platform won't slow down your development cycles, 60% of all Veracode's static assessments finish in less than 10 minutes, 88% in less than 1 hour, and more than 95% are ready within 4 hours. All our customers benefit from the knowledge that comes with assessing over 19 trillion lines of code. With each new scan, the platform gains institutional knowledge which it calls-upon for future assessments.
- **People**: The security industry faces a significant skills gap – there aren't enough security experts. Working with Veracode you gain access to some of the top security experts in the industry. These experts can offer strategic advice for building a scalable and program, help execute the program, and then provide remediation coaching for when flaws are found. In 2015 Veracode's security experts helped fix 70% of all vulnerabilities found, from read-out calls alone customers saw a 2.5X improvement in remediation.

Veracode was founded in 2006 by a world-class team of application security experts from @stake, Guardent, Symantec, and VeriSign. The core technology of our on-demand service was developed in 2002 at the security consultancy @stake to automate application security assessments and now forms the backbone of application risk management from Fortune 500 organizations to mid-market enterprises worldwide.

Veracode has received considerable recognition and awards in the industry including being named a Gartner “Cool Vendor,” The Wall Street Journal’s “Technology Innovation Award,” The Banker’s “Information Security Project of the Year” with Barclays, SC Magazine’s “Best Vulnerability Assessment Solution,” Information Security “Readers’ Choice Award,” and Always On Northeast's "Top 100 Private Company.”

THE VERACODE PLATFORM

The Veracode Application Security Platform provides a holistic, scalable way to manage security risk across your entire application portfolio. We offer a wide range of security testing and threat mitigation techniques, all hosted on a central platform, so you don’t need to juggle multiple vendors or deploy tools. In addition, because application security cannot be solved with technology alone, our security program managers work with you to define policies and success criteria, so you’ll have a strategic, repeatable way to tackle your application security risk. Finally, Veracode educates developers with actionable results, one-on-one coaching and a variety of training, so they can effectively fix existing flaws and code securely moving forward.

Veracode can scan all of the applications and components you build or buy, covering all major languages, frameworks and application types. The Veracode Application Security Platform gives you a central repository for your applications and components, so you have full visibility into your risk posture. In addition, detailed reports and executive-level views help you to prioritize fixes, show reduced risk over time or compare progress across different teams. You also have the flexibility to leverage existing policies or create custom policies and then centrally view policy compliance.

Veracode offers all major types of automated and manual risk assessments (SAST, SCA, DAST and MPT), so you won’t have to juggle multiple vendors, reports and technologies. By integrating into each stage of your software development lifecycle, Veracode helps you build secure software, rather than making costly last-minute fixes that delay releases. We even help you detect and block exploitation attacks in production.

With over 10 years of experience and $100m in investment, the Veracode Platform is used by over 185,000 security professionals and software engineers to mitigate application security risk. Because the Platform has been cloud-based since its inception, it’s constantly learning, so you benefit from solid results with a low false positive rate. These are just a few of the reasons why Veracode has been named a leader in the Gartner Magic Quadrant for Application Security Testing three years in a row.

Many testing tools produce reports with lists of flaws and no actionable information in sight. In contrast, Veracode is dedicated to making sure that you actually fix the flaws

you find. Our security program managers work with you to define policies and success criteria to set up a strategic, repeatable process. Veracode has assisted some of the world’s largest and most complex companies overcome the hurdles preventing

widespread adoption of application security best practices — so you know you're in good hands.

Veracode offers a variety of developer enablement technologies and services to match anyone's learning style. Developers see which line of code their flaw is in and have easy access to short instructional videos to help them fix it. When developers get stuck, they can schedule a one-on-one coaching call with a Veracode application security consultant with a background in development. Veracode also offers application security training through on-demand eLearning courses and instructor-led trainings.

Scan one application or thousands; Veracode works with both the largest enterprises in the world and small development shops. Our cloud- based platform is ideal for fragmented business units and global teams of software engineers.

PRODUCT OFFERING SUMMARIES

Veracode Static Analysis - Manage application security risk in a simple, strategic, scalable way.

Veracode Static Analysis enables your developers to quickly identify and remediate application security flaws without having to manage a tool. Thanks to our SaaS-based model, we increase accuracy with every application we scan. Veracode's patented technology analyzes major frameworks and languages without requiring source code, so you can assess the code you write, buy or download, and measure progress in a single platform. By integrating with your SDLC tool chain and providing one-on-one remediation advice, we enable your development team to write secure code. The Developer Sandbox feature enables engineers to test and fix code between releases without impacting their compliance status.

Pipeline Scan – Make Security part of your CI Pipeline.

As part of the Veracode Static Analysis product Pipeline Scan integrates into your CI Pipeline to provide high speed analysis and feedback for security defects in your code. Leveraging our proven, and highly accurate static engine, Pipeline Scan offers rapid results and scales to your needs. With Pipeline Scan, find issues early, reduce development and remediation costs, and release your code on time – at the speed of your DevOps process.

IDE Scan - Get Secure Coding Feedback in Seconds – Right in Your IDE.

As part of the Veracode Static Analysis product IDE Scan finds security defects in your code and provides contextual remediation advice to help you fix issues in seconds, right in your IDE. Leveraging our proven, and highly accurate static engine, IDE Scan offers immediate results and scales to your needs. You do not need to provision any servers or tune the engine. It simply scans in the background and provides accurate and actionable

results, without taking up resources on your machine. With IDE Scan, find issues early, reduce development and remediation costs, and release your code on time – at the speed of your DevOps process.

Veracode Software Composition Analysis – Secure your usage of Open Source Components.

Veracode Software Composition Analysis analyzes your applications to create an inventory of third-party commercial and open source components, alerting your developers to the presence of components with known vulnerabilities. When a new component vulnerability is exposed, you can quickly identify if any of your applications are at risk, so you can proactively take action.

Veracode Dynamic Analysis - Discover and assess risk of thousands of corporate websites.

Veracode Dynamic Analysis (DA) offers a unified solution to find, secure, and monitor all your web applications – not just the ones you know about. First, Veracode discovers and inventories all your external web applications, then performs a lightweight scan on thousands of sites in parallel to find critical vulnerabilities and helps you prioritize your biggest risks. As a second step, you can run authenticated scans on critical applications to systematically reduce risk while continuously monitoring your security posture as part of the SDLC. Veracode offers multiple scanning technologies on a single platform, so you get unified results, analytics, and increased accuracy.

Veracode eLearning – Improve Developer Security Knowledge

Veracode eLearning empowers software developers, testers and security leads to develop secure applications from inception to deployment, providing the critical skills they need to identify and address potential vulnerabilities. By using web-based training offered through the Veracode Application Security Platform, customers can quickly onboard all employees, including geographically diverse development teams, with the security knowledge needed to prevent a potential breach and meet compliance requirements. Content is available via contextual recommendations when fixing vulnerabilities or on demand, and the security team can easily track and monitor student progress. Veracode Security Training meets requirements for PCI-DSS section 6.5 and other compliance initiatives requiring developer secure coding training, and can be used for continuing education credits

Veracode Security Labs – Hands on Secure Code training

Veracode Security Labs shifts application security knowledge left, training developers to tackle evolving modern by exploiting and patching real code, and applying DevSecOps principles to deliver secure code on time. Through hands-on labs that use modern web apps written in your chosen languages, developers learn the skills and strategies that are directly applicable to your organization's code. Detailed progress reporting, email

assignments, and a leaderboard encourage your developers to continuously level up their secure coding skills.

CUSTOMER SUCCESS PACKAGE SUMMARIES

Strong security means more than having powerful technology. Our services help developers rapidly identify, understand and remediate critical vulnerabilities — and help transform decentralized, ad hoc application security processes into ongoing, policy-based governance.

Veracode Security Program Management - Ensure quick successes with experienced security program management and scale your application security program without adding headcount.

Veracode Security Program Management (SPM) helps enterprises map out their strategy and deliver results with. Veracode has been involved with thousands of application security programs over the past 10 years. We help you with security program readiness and execution, so you don't have to find and retain highly specialized talent. As a result, we see customers who use Veracode SPM grow their application coverage by 25% each year, decrease their time to deployment and achieve better scan and remediation metrics. Most importantly, our security program managers ensure that your program stays on track to meet your strategic goals.

Veracode Remediation Advisory Solutions - Get an application security expert to advise your development teams and benefit from a deeper vulnerability analysis with dedicated consultants.

Veracode Remediation Advisory Solutions (RAS) provide application security experts with a development background that act as a "personal trainer" for your engineering team. Unlike services that assign different resources for each vulnerability, the same Veracode RAS consultant will work on all vulnerabilities of a specific application to provide a deeper level of analysis and so you don't have to start from square one on each call. Your developers will learn secure coding practices in their environment and process, decreasing the number of flaws over time, leading to cost savings for you and your organization.

Veracode Developer Training - Grow your developers' skills and become more secure in the process.

Remediate 30% more vulnerabilities with developer training and Reduce costs by trained Veracode Developer Training empowers developers, testers and security leads to develop secure applications, providing the critical skills they need to identify and address potential vulnerabilities. Veracode offers three styles of teaching that reinforce each other. Instructor-led training offers real- time training that's tailored to your organization. On-demand training is integrated with the Veracode Application Security

Platform and allows developers to learn when and where they need it. And just-in-time training offers refreshers and contextual recommendations to help developers fix vulnerabilities. Development organizations that leverage Veracode eLearning see a 30 percent higher vulnerability fix rate by training developers on application security.

PRICING

The Veracode Analysis Technologies are licensed on an Annual Subscription based upon the number of Applications being tested. For Static Analysis there are provisions for Small (under 1MB), Standard (1MB to 300MB) and Large (over 300MB) applications. Indicative pricing based on 10 applications is as follows:

Description	List Price		# of licenses	Volume Discount	Total Cost per Year	
	3 Year	1 Year			3 Year	1 Year
Veracode Static Analysis						
Small	$2,000	$2,200	10	15%	$17,000	$18,700
Standard	$10,000	$11,000	10	15%	$85,000	$93,500
Large	$20,000	$22,000	10	15%	$170,000	$187,000
Veracode Software Composition Analysis						
Standalone	$3,000	$3,300	10	15%	$25,500	$28,050
With Static	15% of Static Price					
Veracode Dynamic Analysis						
Per URL	$2,000	$2,200	10	15%	$17,000	$18,700
With Static	25% of Static Price					
Veracode Discovery						
Single Scan	$2,727	$3000	10	15%	$23,182	$25,500
Unlimited Scans	$90,909	$100,000	1	15%	$90,909	$100,000

The Veracode Education offerings are licensed on an Annual Subscription based upon the number of Users. Indicative pricing is as follows:

Description	List Price	# licenses	Volume Discount	Total Cost per Year
Veracode eLearning				
Application Security Track	$250	10	10%	$2,250
Security Awareness Track	$100	10	10%	$900
Inspired eLearning Track	$80	10	10%	$720
Veracode Security Labs				
Security Labs	$750	10	10%	$6,750

Veracode Services including Technical and Program support are priced based on the Analysis Technologies and Education offerings that are purchased. There are 3 levels of support available: Standard, Premier and Premier Plus:

Description	Pricing
Technical and Program Support - Standard	10% of SaaS Product List Price
Technical and Program Support – Premier	20% of SaaS Product List Price
Technical and Program Support – Premier Plus	27% of SaaS Product List Price

SERVICE LEVELS AND RESILIANCE

Veracode's Business Continuity and IT Disaster Recovery plans provide structure and guidance to ensure that all departments and business functions have in place robust and current continuity and recovery plans that are regularly reviewed and tested.
The plans provide for the prompt and effective continuation of all business critical functions and service offerings in the event of a disruption of service.
Veracode will take all reasonable steps to ensure that in the event of a service interruption, essential services will be maintained, and normal services restored as soon as possible.

Each department and business function within Veracode generally perform risk assessments and business impact analyses to determine the criticality of their department and business function, and document the risk their loss would pose to the company.

Business Continuity Plan

Veracode's business operations are performed at our Corporate Offices in Burlington, MA. However, Veracode personnel routinely work remote due to personal or weather related reasons. This remote-work capability is the foundation of our Continuity Plan in the event of a business interruption at the Corporate Offices.

Veracode uses Send Word Now as our critical Incident alerting and messaging system to notify employees of business interruptions.
Critical elements of the infrastructure supporting the corporate office is located in the Lowell and Somerville facility. This includes email and messaging systems as well as a VPN for remote connectivity.
Veracode's phone system is provided as a service from 8x8 communications and is accessible to employees anywhere they are located.

Backup/Recovery and Data Protection Plans

Veracode has a comprehensive data protection plan and the Veracode platform has multiple levels of protection to ensure service continuity. The platform is redundant at each level and critical data backed up and maintained offsite. A warm backup site is in place for or the unlikely extended outage requiring restoration of services in an alternative location.

The Veracode platform has built-in redundancies at each level of its service infrastructure that is hosted at third party service providers and that includes network, web, application & database tiers.

Veracode protects data required for the Veracode Application Security Platform (VASP) to function, including system data and infrastructure data.

Backups of customer metadata are performed incrementally throughout the day and encrypted with 128-bit AES before being transmitted to off-site storage daily.

For security reasons customer binaries are not backed up. In the event of a disaster occurring to the hosting facility, customers will only have to re-upload their binaries for any scans that were in process.

If the primary hosting site is no longer operational, the Veracode services will be restored at our warm backup site. The fail-over location is at Veracode's alternate processing site.
Equipment to support all tiers of operations are maintained and kept up to date in the alternate facility. Such an arrangement would be temporary and provide for the restoration of a reduced scale of service. Full resumption of services can be achieved at the primary facility if available; or relocated to an alternate processing location when available.
This includes redundant firewalls, switches, load balancers, web servers, application servers, database servers, engine hosts, and data storage clusters. Operations can be resumed once the current data is restored from a backup and the external DNS entry is changed to point to the new location.

Disaster Recovery Preparedness

Disaster recovery testing and exercises are conducted to demonstrate the recoverability of services with a defined RTO (72 Hours) and RPO (24 Hours).
Throughout the year the Veracode IT organization undertakes a number of tests and drills to enhance its preparedness in case of a disaster.

Service Incident Reporting

In addition to formal DR testing procedures, a Service Incident Report (SIR) Process exists to review and document any significant issues in our production environment. This can result in changes to the Business Continuity and IT Disaster Recovery Plan throughout the balance of the year, with an improved posture relative to the identification of incidents as well as incident response.