

## Serious About Delivering Secure SaaS Solutions

Organizations of all types depend on Veracode to analyze mission-critical, confidential applications. Veracode is serious about ensuring the security and confidentiality of our customers' binaries.

## Introduction

Veracode is entirely focused on solving security problems. We recognize that security problems are more efficiently resolved by using the elastic capacity, rapid feature deployment and continuous improvement capabilities enabled by cloud computing. Yet we also recognize that customers should not be forced to choose between innovative solutions and secured use of solutions. Therefore, Veracode had to solve the problem of delivering cloud-based services securely to customers and ensuring that customer binaries, bytecode and analysis results remain confidential.

Veracode was founded by leaders in the security industry who have been solving customer security problems at such companies as @stake, Guardent, VeriSign, and Symantec. We have leveraged our experience with securing customer networks, applications and data to design, implement, maintain and audit security at every layer of our cloud-based services. This paper outlines the mechanisms and procedures we have taken to deliver our secured cloud-based services.

## Comprehensive security auditing at every level



Veracode believes auditing is critical for proactively maintaining secured services. We have a three pronged approach to security auditing.



We use the Veracode platform to perform dynamic and static analysis on any changes we make to our software binaries. Binary analysis creates a behavioral model by analyzing an application's control and data flow through executable machine code – the way an attacker sees it. Unlike source code tools, this approach accurately detects issues in the core application and extends coverage to vulnerabilities found in 3rd party libraries, pre-packaged components, and code introduced by compiler or platform specific interpretations. We use this analysis to complete our own ongoing threat assessments and rapidly deploy security technologies at every infrastructure layer as appropriate.

Our platform is hosted at a secure datacenter facility at Sungard. Sungard has been certified as an SSAE 16 Type II SOC I facility (formerly known as SAS-70). This certification is performed on an annual basis. Learn more about SSAE 16 at <http://www.ssaе-16.com/>

Veracode has passed the rigorous annual SysTrust certification process by Ernst & Young to ensure we have appropriate internal controls in place for security and confidentiality of our environment. The audit verifies that Veracode maintains effective controls over its on-demand platform to protect information designated as confidential as committed or agreed.

Learn more about:

- SysTrust and its security and confidentiality criteria at <http://www.webtrust.org/>
- The full Veracode's SysTrust report at [https://cert.webtrust.org/pdfs/veracode\\_systrust.pdf](https://cert.webtrust.org/pdfs/veracode_systrust.pdf)

## Protection at the application level



Veracode's cloud-based platform uses role-based access control (RBAC) to provide a robust and flexible security model to govern access to customers' content. Fine-grain access control provides a powerful least-privilege model to ensure that users only have access to the data necessary to perform their required job functions. Access control is enforced across multiple layers of the platform and is continuously evaluated throughout the user session.

Veracode offers two-factor authentication to provide customers a higher degree of authentication and control. Two-factor authentication is also required for all Veracode employees that are allowed access to the Platform. Absolutely no shared use of accounts is allowed and passwords must conform to best practice guidelines. Finally, login sessions automatically time out and require authentication to re-establish.

## Protection at the data level



All binaries in transit to the Veracode service are protected by SSL or VPN connections using strong encryption methodologies and digital certificates signed by all delivery systems. Veracode generates a private key using a pristine, non-networked host and is adequately protected during its lifespan.

All customer files are encrypted with a unique key per application using 128-bit AES encryption and stored in a file share. From this point forward, the files are never decrypted to disk; decryption for the purpose of analysis is performed only in memory by the scanning process. Unique application keys are stored securely also with 128-bit AES encryption. As a result no one with access to the file share or system backups can access an unencrypted copy of sensitive customer data.

All data submitted for analysis by a customer is owned by the customer. Veracode access to customer data is limited to authorized security personnel within the Center for Software Assurance (CSA) to perform quality assurance and enhanced security analysis. Physical access to the CSA is controlled by a key card system. Only authorized employees who have undergone background checks and require this level of access to perform their job responsibilities are issued CSA key cards. Network connectivity of workstations in the CSA is limited to the platform. Further, all customer data interaction by Veracode personnel is recorded in audit files. Video cameras are installed inside the CSA and activity is monitored.

Veracode automatically purges the encrypted binaries from our storage devices 90 days after the application scan results are delivered. Binaries are deleted in compliance with C2/Military security standards (DoD 5220.22-M) utilizing a triple pass/wipe strategy. The retention policy is configurable in that customers can request retention periods as short as 30 days.

## Protection at the network level



Veracode's service network is protected by multiple security systems to provide layered defense. A combination of external firewalls, internal firewalls and intrusion detection systems monitor network activity. All traffic between the Veracode service and the customer is protected by SSL or VPN

connections using strong encryption methodologies and digital certificates signed by all delivery systems.

Periodic network vulnerability assessments are also performed using third party assessment tools, and identified vulnerabilities are remediated. Industry standards for proactive monitoring, logging and analysis of security events have been implemented, including:

- Traditional antivirus software to repel basic attack signatures
- Stateful inspection firewalls to filter unauthorized inbound network traffic
- Network-based intrusion detection systems to monitor traffic patterns and known vulnerabilities for potentially malicious activity.

## Protection at the facilities level



Our production infrastructure resides in a world-class SAS 70 Type II certified and audited datacenter. This facility implements 24/7/365 monitoring and surveillance and on-site security staff. Only authorized personnel are allowed physical access to the hardware which is protected by a strict access controls including two-factor cryptographic cards, biometric systems and mantraps.

Continuous datacenter operation is ensured by multiple power feeds, UPS devices and backup generators. Servers are hosted in redundant facilities, which are automatically backed up to a geographically-separated site with similar access controls. Only customer metadata is backed up off-site. In the event of a datacenter disaster, any pending scans will require that their binaries be re-uploaded to the failover datacenter. Backups of customer metadata are encrypted with 128-bit AES before being transported off-site for storage. As a result no one with access to the backup systems can access an unencrypted copy of sensitive customer data.

All systems within the service platform are set up and managed by experts according to industry best practices where hardened configurations are used to limit unnecessary attack vectors. All configuration activity follows a formal process that encompasses documentation, testing, and approval. Only authorized personnel are allowed to set up and manage platform systems. Operating system patches are monitored and applied as necessary to maintain the highest level of security.

## Protection during the production deployment process



Rigorous testing of all systems is performed before going into production. All testing is done in the QA and staging environments. Veracode completes both static and dynamic testing during QA and staging phases, and penetration testing is done using both internal and external resources to broaden coverage. We monitor and validate that platform configurations are accurately maintained as the platform moves from QA to staging to production. These measures help ensure expected results when deploying to production. The production deployment process is governed by a set of documented release procedures that must be followed by authorized personnel.

# VERACODE

WHITE PAPER

## VERACODE

*Software Security Simplified*

Veracode, Inc.  
4 Van de Graaff Drive  
Burlington, MA 01803

Tel +1.781.425.6040  
Fax +1.781.425.6039

[www.veracode.com](http://www.veracode.com)

© 2012 Veracode, Inc.  
All rights reserved.

### ABOUT VERACODE

[Veracode](#) is the only independent provider of cloud-based [application intelligence](#) and [security verification](#) services. The Veracode platform provides the fastest, most comprehensive solution to improve the security of internally developed, purchased or outsourced software applications and third-party components. By combining patented static, dynamic and manual testing, extensive eLearning capabilities, and advanced application analytics, Veracode enables scalable, policy-driven application risk management programs that help identify and eradicate numerous vulnerabilities by leveraging best-in-class technologies from [vulnerability scanning](#) to [penetration testing](#) and [static code analysis](#). 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. Veracode works with global organizations across multiple vertical industries including Barclays PLC, California Public Employees' Retirement System (CalPERS), Computershare and the Federal Aviation Administration (FAA). For more information, visit [www.veracode.com](http://www.veracode.com), follow on Twitter: [@Veracode](#) or read the [Veracode Blog](#).