

Veracode's Security Approach

Veracode is first and foremost a security company solving a security problem. We do so in a fundamentally different and better way by delivering innovative application security services in the cloud. We recognize that data security and confidentiality is top of mind for our customers. So, we have developed a state-of-the-art security infrastructure that allows you to take advantage of our cloud platform with the peace of mind that comes from knowing your data is in safe custody.

Veracode Security

- Physical Security
- Perimeter Security
- Platform Application Security
- Internal Security
- User Authentication
- Data Security Standards
- System Configuration
- Testing and Validation
- Independent Third Party Certification

Veracode is Security

Veracode was founded by leaders in the security industry such as @stake, Guardent, VeriSign, and Symantec—companies well known for their expertise in application security, information security, and managed services. We leveraged this domain knowledge to build a comprehensive security infrastructure and program. Security is built into every stage of the software development lifecycle (SDLC) and beyond, from design to deployment, and includes constant monitoring and continuous improvement.

Physical Security

Our production infrastructure is located in Marlborough, MA at a world-class SAS 70 Type II certified datacenter. This facility implements stringent 24-hour physical security controls. Access to the production servers is protected by biometric scanners, man-traps, and card key readers. Only authorized personnel are allowed physical access to the hardware. The entire facility is monitored by security cameras and full records of any physical access are maintained. Service audits are performed periodically with Type II reports issued every six months.

Perimeter Security

Veracode's service network perimeter is protected by multiple security systems to provide defense in depth. A combination of external and internal firewalls and intrusion detection systems, sourced from industry-leading vendors, protect and monitor activity at the perimeter. All traffic between the Veracode service and the customer is limited to Secure Socket Layer protocol.

Security monitoring on the Veracode service is performed at each layer of technology, including network, operating system, application, and database layers. Configuration standards have been implemented for logging and monitoring security events.

Monitoring includes antivirus software with automatic virus signature updates, stateful inspection firewalls to filter unauthorized inbound network traffic, custom monitoring for application security related events and network intrusion detection systems to monitor traffic patterns and known vulnerabilities for potentially malicious activity. Periodic network vulnerability assessments are also performed proactively using third party assessment tools, and identified vulnerabilities are remediated.

Veracode Platform Application Security

Veracode's cloud platform uses role-based access control (RBAC) to provide a robust and flexible security model to govern access to your 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. Finally, customer Intellectual Property is destroyed when analysis is completed using secure deletion and overwriting of disk space. Periodic application vulnerability assessments are also performed, and identified vulnerabilities are remedied.

Internal Security

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.

User Authentication

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.

Data Security Standards

Data security is central to the design of the platform. It protects your data and limits access according to industry standards of good practice such as the Payment Card Industry (PCI) Data Security Standard. The PCI standard is designed to protect data from both internal and external attacks. Veracode believes that your information must be guarded with those same rigorous standards to prevent unauthorized data access. Inside attacks can be even more difficult to prevent. We have implemented a set of advanced database technologies to prevent back door data access by operations personnel with administrative privileges.

Veracode addresses the security needs of data in transit and at rest:

- to ensure the confidentiality of your information, all data in transit with the Veracode service is limited to SSL or VPN connections using strong encryption methodologies and is automatically certificate signed by all delivery systems; and
- all sensitive data at rest is stored in an encrypted format. This includes general purpose files and database content. Multiple encryption keys are used to ensure proper segregation of data between customer datasets. All backups are encrypted to prevent the possibility of unwanted data access in the event of lost or stolen media.

System Configuration

All systems within the service platform are setup 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.

Testing and Validation

Rigorous testing of all systems is performed before going into production. All testing is done in the QA and staging environments where we maintain a complete copy of the production infrastructure. We have a suite of tools used to validate that platform configurations are properly maintained from one environment to the next. These measures help ensure expected results when deploying to production. Our testing methodology includes functionality as well as security. Penetration testing is done using both internal and external resources to broaden coverage. The production deployment process is governed by a set of documented release procedures that must be followed by authorized personnel.

Independent Third Party Certification

Our platform is hosted at a secure processing facility at Sungard. This facility has obtained a number of security certifications including a SAS 70 Type II which is performed on a bi-annual basis. In addition to this Veracode has passed a rigorous Systrust certification process by Ernst & Young to further augment the security and confidentiality of our customer's information and our infrastructure.

VERACODE

Veracode, Inc.
4 Van de Graaff Drive
Burlington, MA 01803
Tel +1.781.425.6040
Fax +1.781.425.6039
www.veracode.com

© 2011 Veracode, Inc.
All rights reserved.
DSSA/2011