Service Organization Control 3 Report

Veracode Application Security Services System

Description relevant to *Security*, *Availability* and *Confidentiality* for the period April 1, 2017 to March 31, 2018

Table of Contents

OCDTECH

A Division of O'Connor & Drew, P.C.

25 Braintree Hill Office Park, Suite 102, Braintree, MA 02184 • Phone: (844) OCD-TECH • Fax: (617) 472-7560 •
https://www.ocd-tech.com

Report of Independent Accountants

To the General Manager CA Veracode

Approach:
We have examined management's assertion that CA Veracode (Veracode) maintained effective controls to provide reasonable assurance that:

- the Application Security Services System was protected against unauthorized access, use, or modification to achieve Veracode's commitments and system requirements
- the Application Security Services System was available for operation and use to achieve Veracode's commitments and system requirements
- the Application Security Services System information is collected, used, disclosed, and retained to achieve Veracode's commitments and system requirements

during the period April 1, 2017 to March 31, 2018 based on the criteria for security, availability and confidentiality in the American Institute of Certified Public Accountants' TSP Section 100A, *Trust Services Principles and Criteria, for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. This assertion is the responsibility of Veracode's management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of Veracode's relevant security, availability and confidentiality policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Veracode's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program***.***

Inherent Limitations:
There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its internal control, those controls may provide reasonable, but not absolute, assurance that its commitments and system requirements related to security, availability and confidentiality are achieved.

Examples of inherent limitations of internal controls include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity. Furthermore, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion:
In our opinion, Veracode's management's assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria for security, availability and confidentiality.

O'Connor & Drew, P.C.

July 2, 2018

Report by Management on the Controls over the Application Security Services System based on the AICPA Trust Services Principles and Criteria for Security, Availability and Confidentiality

July 2, 2018

We, as management of CA Veracode are responsible for designing, implementing and maintaining effective controls over the Application Security Services (System) to provide reasonable assurance that the commitments and system requirements related to the operation of the System are achieved.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in Security controls, an entity may achieve reasonable, but not absolute, assurance that all security events are prevented and, for those that are not prevented, detected on a timely basis.

Examples of inherent limitations in an entity's Security's controls include the following:

- Vulnerabilities in information technology components as a result of design by their manufacturer or developer
- Ineffective controls at a vendor or business partner
- Persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity

We have performed an evaluation of the effectiveness of the controls over the system throughout the period April 1, 2017 to March 31, 2018, to achieve the commitments and system requirements related to the operation of the System using the criteria for the security, availability and confidentiality (Control Criteria) set forth in the AICPA's TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. Based on this evaluation, we assert that the controls were effective throughout the period April 1, 2017 to March 31, 2018 to provide reasonable assurance that:

- the System was protected against unauthorized access, use, or modification to achieve Veracode's commitments and system requirements
- the System was available for operation and use, to achieve Veracode's commitments and system requirements
- the System information is collected, used, disclosed, and retained to achieve Veracode's commitments and system requirements

based on the Control Criteria.

Our attached description of the boundaries of the Application Security Services System identifies the aspects of the Application Security Services System covered by our assertion.

Paiman Nodoushani
SVP Products

System Description of Veracode's Application Security Services System

Overview of CA Veracode

CA Veracode, now part of CA Technologies, enables the secure development and deployment of the software that powers the application economy.

With its combination of automation, process and speed, CA 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 are able to fully realize the advantages of DevOps environments while ensuring secure code is synonymous with high-quality code.

CA Veracode serves more than 1,400 customers worldwide across a wide range of industries. The CA Veracode Platform has assessed more than 2 trillion lines of code and helped companies fix more than 27 million security flaws.

Learn more at www.Veracode.com, on the CA Veracode blog and on Twitter.

Veracode Application Security Services System

The Veracode Application Security Services System is designed to assist organizations in verifying an application's security state and in determining acceptable levels of risk before the software is deployed for business use. In conjunction with providing these services, Veracode relies upon its Center for Software Assurance (CSA) function to perform quality review procedures over the results generated by the Veracode Application Security Services System prior to delivering them to its clients. The Veracode Application Security Services System is comprised of the systems and services noted below.

Cloud-Based Platform ("Platform")

The Veracode cloud-based platform, which resides on Veracode's private cloud, provides a centralized way for customers to secure web, mobile and third-party applications across their global infrastructure throughout the system lifecycle without slowing innovation.

The traditional, on-premises approach to application security may not adequately address pervasive application-layer risk across global enterprises. Unnecessary complexity for rapidly-moving development teams and a decentralized model presents challenges to consistently apply policies, reporting and metrics.

The Veracode cloud-based approach is fundamentally different. It is simpler and more scalable, to help systematically reduce application-layer risk across our customers' entire global software infrastructure. The Platform is comprised of the following characteristics:

Central Policy Manager

The Central Policy Manager enables enterprises to define and enforce uniform security policies across their applications, including third-party software (such as outsourced applications and third-party libraries), business units, and development teams in their organizations.

Security Analytics & Peer Benchmarking

The Platform provides a suite of analytical dashboards to provide customers with a fast and comprehensive way to track their application security program and to compare their security posture to industry peers.

The dashboards analyze results from tens of thousands of applications and millions of lines of code scanned by the Veracode cloud-based platform to help better understand the threat space and quantitatively compare the security of applications against industry peers.

Compliance Workflow Automation

The Veracode cloud-based platform assesses applications for compliance with common compliance frameworks and industry standards, such as PCI, the OWASP Top 10, the CWE/SANS Top 25, HIPAA and NIST 800-53 and allow customers to customize policies to support specific audit requirements.

Role-Based Access Control

The Platform utilizes role-based access control to help enable user organizations securely upload and scan binaries, scan web applications, and view results and metrics.

Veracode and customer users are assigned to specific roles with pre-defined permissions, with eleven distinct roles defined.

APIs & Plugins

To help maximize developer productivity and adoption, the Platform helps integrate security analysis into existing workflows with application program interfaces (APIs) and plug-ins.

Products

Binary Static Analysis (SAST)

Static Application Security Testing (SAST), or “white-box” testing, finds common vulnerabilities by performing a deep analysis of applications without actually executing them.

Unique in the industry, the Veracode patented binary SAST technology analyzes all code, including open source and third-party components, without requiring access to source code and the SAST is designed for agile development processes.

SAST supplements threat modeling and code reviews performed by developers, to help find coding errors and omissions more quickly and at lower cost via automation. Customers typically run the scans in the early phases of the Software Development Lifecycle, as it is easier and less expensive to fix problems before going into production deployment.

Software Composition Analysis

Software Composition Analysis enable developers to continuously audit their code, including third-party and open source components, to help identify vulnerabilities and offer remediation assistance and advisory services for all impacted applications.

Dynamic Analysis (DAST)

Also known as "black-box" testing, Dynamic Application Security Testing (DAST) helps identify architectural weaknesses and vulnerabilities in web applications before cyber criminals can find and exploit them both before and after the applications have shipped.

DynamicDS

DynamicDS (Deep Scan) helps identify vulnerabilities, both with and without access credentials, including known critical vulnerabilities that are easy to find and exploit in the OWASP Top 10 and the CWE/SANS Top 25 through a highly-automated approach.

DynamicDS leverages results from baseline DynamicMP assessments to help understand where to focus deep-scan assessments and then feeds this security intelligence to existing Web Application Firewalls (WAF) for rapid mitigation via virtual patching.

Virtual Scan Appliance (VSA)

The Virtual Scan Appliance (VSA) is a pre-configured virtual appliance that implements the Veracode DynamicDS (Deep Scan) engine to probe web applications behind customers' firewalls to help identify vulnerabilities that can be exploited not only by malicious insiders but also from outsiders who gain credentialed access to internal systems.

Web Application Perimeter Monitoring

Many enterprises do not consistently maintain an inventory of public-facing applications. To help reduce the global application threat surface, the Veracode parallel cloud infrastructure discovers customers' public-facing applications and helps identify the most exploitable vulnerabilities.

Discovery

Discovery helps to create a global inventory of customers' externally-facing web applications including related sites (info, mail, etc.) and mobile sites. This cloud-based platform uses production-safe application-layer crawling and an auto-scaling cloud infrastructure to discover potential sites daily.

DynamicMP

Dynamic MP helps baselines application risk by identifying highly exploitable vulnerabilities, such as those found in the OWASP Top 10, and mitigate them via WAF integration along with actionable feedback for developers. The system leverages the parallel cloud infrastructure to inspect thousands of web applications simultaneously with lightweight, non-authenticated scans.

Dynamic scanning complements other techniques such as static application security testing and manual penetration testing to find vulnerabilities in web applications at runtime. The Veracode end-to-end solution starts with discovery, proceeds to baseline scanning of applications in parallel, continues with scanning and enables continuous, ongoing monitoring to maintain security posture.

eLearning

Help foster a higher level of security awareness and proficiency among developers with comprehensive training delivered via the Veracode cloud-based platform and help address compliance requirements, such as PCI-DSS Requirement 6.5, ISO and SANS Application Security Procurement Contract Language, and embed security best practices into the Software Development Life-Cycle to rapidly address compliance requirements.

Services

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

Remediation Coaching

Veracode’s services help developers efficiently incorporate secure coding skills and practices into their existing development processes. Veracode has assisted development teams overcome their resistance to changes required to develop secure code.

Developer Coaching

Veracode’s specialized services help developers understand assessment results, prioritize remediation efforts and integrate with existing SDLC tools and processes.

Program Management

Veracode’s Security Program Managers (SPMs) enable the end-to-end success of a Client’s global application security program. Veracode’s Program Managers help Clients implement enterprise-wide governance models and day-to-day tactics to systematically reduce risk from application-layer attacks, based on industry wide best practices and addresses risk associated with third parties.

Penetration Testing

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

Reducing false negative (FN) rates in the most critical applications requires a combination of multiple techniques, including SAST, DAST and manual penetration testing.

The Veracode cloud-based platform provides a single central location for consolidating results from these multiple techniques, as well as for sharing results across multiple teams and evaluating risk using a consistent set of enterprise-wide policies.

Third-Party Security

Veracode's third-party security services help ensure that applications comply with enterprise security policies and industry standards, such as the OWASP Top 10 and PCI.

Vendor Application Security Testing (VAST)

VAST helps reduce the risk associated with third-party software, so you can innovate with more speed and confidence than ever. With VAST, Veracode manages the entire third-party program for you as a cloud-based service and work directly with vendors in the software supply chain to help ensure they are compliant with corporate security policies.

Supply Chain Security

Vendor Application Security Testing (VAST) reduces the risk associated with third-party software. With VAST, Veracode manage the entire third-party program for a Client as a cloud-based service — and work directly with vendors in a Client's software supply chain to ensure they are compliant with corporate security policies.

Independent Audit Service

With the increasing focus on third-party software risk by major industry groups, software suppliers are now being asked to provide independent attestation that their applications have been tested for resilience against security standards and corporate policies. The Veracode Independent Software Audit service provides a simple and cost-effective way to give enterprise customers the third-party security attestation they require. As a result of the Veracode patented binary static analysis, customers do not need to upload their source code to the Veracode cloud-based platform, protecting intellectual property.

VerAfied Directory

For software customers (e.g. ISVs with public applications, software as a service), binary static scans can be run to identify vulnerabilities. The customer can the re-run the scan, if necessary, and once any vulnerabilities are remediated, receive the VerAfied security mark. The VerAfied security mark helps demonstrate processes are in place to help vulnerabilities from software and to comply with industry standards like the OWASP Top 10 or the CWE/SANS Top 25 Most Dangerous Software Errors.

Components of the System

Collectively, the Veracode Application Security Services System consists of the following components:

Software

Cloud-Based Platform ("Platform")

The Platform, developed in-house and managed by Veracode, is responsible for supporting certain aspects of Veracode's services provided to customers, including application submission, job scheduling, establishing user accounts, generating notifications, client reporting, and collaborative remediation of application security flaws. The Platform system's architecture is supported by the following software components:

- Application Server: JBoss
- Web Servers: Tomcat and Apache
- Database: Oracle, Microsoft SQL Server and MySQL
- Operating Systems: Solaris/Windows/CentOS Linux, Virtual Host

The Virtual Scan Appliance (VSA) is an Open Virtual Appliance (OVA) qualified to run in virtualization platforms supporting the Open Virtualization Format (OVF). The VSA is a virtual appliance that enables dynamic application security testing. The VSA is integrated into the Cloud-Based Platform for workflow, policy management and reporting giving customers a single location for managing security.

Infrastructure

The technology infrastructure supporting the Veracode Application Security Services System resides primarily within data center facilities hosted by third party service providers, Sungard Availability Services ("Sungard"), in Somerville, Massachusetts and Amazon Web Services (AWS), within US availability zones. As part of Veracode's internal controls, Veracode management has designed and implemented policies and procedures that monitor activities performed by Sungard and Amazon Web Services, including physical security, logical security and change management.

The production hardware supporting the Veracode Application Security Services System includes equipment from the following vendors: Oracle, Hewlett Packard, NetApp, F5, Check Point, and Cisco.

Certain technology infrastructure components relied upon to support activities performed by the Center for Software Assurance (CSA) are housed within Veracode's secured corporate datacenter at the headquarters facility in Burlington, Massachusetts. Veracode relies on formal internal control policies and procedures to manage this environment. The production hardware supported in the Veracode datacenter includes equipment for servers and desktops from Hewlett Packard.

The Veracode Application Security Services System's architecture follows an n-tiered design model comprised of web, application, middleware and database layers. Each respective layer and the supporting infrastructure are implemented utilizing server farms and high-availability clustering to eliminate any single point of failure.

People

The following functional groups within Veracode are responsible for supporting the Veracode Application Security Services System:

- Engineering – This group is responsible for the design, development, quality assurance (QA), and performance testing of the Veracode Application Security Services System.
- Production Operations – This group is responsible for the overall production environment and infrastructure, oversight of production software deployment, and coordination of the production engineering activity.
- Center for Software Assurance (CSA) – This group has primary responsibility for performing quality review procedures over the results generated by the Veracode Application Security Services System prior to delivering to clients. The CSA resides in a secure location within the Burlington, Massachusetts headquarters facility.
- Services (Customer Success and Support) – These groups are responsible for customer relationship management, satisfaction and support, along with technical account management and user account management.
- Information Technology – This group is responsible for monitoring and maintenance of the corporate IT infrastructure, Development, QA and Staging environments as well as the infrastructure supporting the system.
- Information Security Oversight Council (ISOC) – The ISOC serves as Veracode's overall governing Information Security body, responsible for providing strategic direction and oversight of the information security program, reviewing and approving changes and monitoring ongoing effectiveness of security policies, procedures and processes applicable to the Veracode Application Security Services System.
- Information Security Assessment Team (ISAT) – The ISAT is a subset of the ISOC and is primarily responsible for coordinating and executing incident response protocols, ensuring compliance with current security procedures and developing changes to existing security and confidentiality policies, procedures, and processes. Security and confidentiality breaches are also reported to this group.
- Product Security Incident Response Team (PSIRT) – The PSIRT is a tactical cross-functional product team who assess immediate and emerging threats to the Veracode

Application Security Services System. PSIRT develops direct tactical response plans (countermeasures) to secure the Veracode Application Security Services System.

- Production Engineering – This group provides management, monitoring, and maintenance of all the production hardware, operating systems, network infrastructure, and database components of the Veracode Application Security Services System.

All teams are recruited and managed using Veracode's policies and procedures.

Procedures

Veracode has documented policies and procedures that support the management, operations, monitoring and controls over the Veracode Application Security Services System. Specific examples of relevant policies and procedures include, but are not limited to, the following:

- Policy management and communication
- System security and administration
- Computer and network operations
- Service application management and administration
- Backup management and processing
- Monitoring and event correlation
- Vulnerability management
- Change management, including release to production processes

Policies and procedures are made available to employees through the Veracode intranet (Wiki) site, reviewed annually by the ISOC and updated where required.

Data

The Veracode Application Security Services System manages customer data stored on an encrypted NetApp storage array, as well as within production databases and devices within the physically secured CSA Workstation area. Customer data files located on the operating system are encrypted using unique keys assigned to each customer application analyzed. Select fields of customer information within the database environments are also stored in encrypted format for enhanced protection. Example of customer information currently maintained by the Veracode Application Security Services System includes:

- Account and user information
- Application metadata
- Application binary files

- Application vulnerability data
- Audit data
- System and application log data

Veracode only retains customer application binary files for a defined period of 60 days within the Veracode Application Security Services System. On a daily basis, a job is run to systematically dispose of any customer binary files that have aged 60 days. In the event another scan of the binary is required, Customers will have to upload the binary file to the tool for analysis. Other customer data is securely retained within the system until Customers request removal.

Additionally, Veracode has a process in which system components, including laptops, workstations and servers, are sanitized to remove any sensitive data prior to being physically removed from the secure Veracode environment. Upon completion of the sanitizing wipe, Veracode receives a certificate from the third-party tool to evidence the process was completed.

Sub-service Organizations

Veracode utilizes Sungard Availability Services and Amazon Web Services (sub-service organizations) to provide data center hosting (Sungard) and cloud-hosting (Amazon) services, including physical security and environmental safeguards, to support the Veracode environment. It is expected that the sub-service organization has implemented the following controls to support achievement of the associated criteria:

Criteria Reference	**Expected Sub-Service Organization Controls**
CC5.4 (Amazon Only)	Access to data, software, functions, and other IT resources is limited to authorized and appropriate personnel.
CC5.5	Access to the data center is restricted to authorized employees and contractors using card readers and other systems (e.g. hand readers).
	Visitors to the data center are required to sign a visitor log.
	Physical access to the data center facilities is restricted to appropriate personnel who require such access to perform their job functions.
	Administrative access to the card system and other systems (e.g. biometric readers) is limited to authorized and appropriate personnel.
	Camera surveillance of the data center is monitored and retained for a period of time.
A1.1 (Amazon only)	Current and future processing capacity is monitored and evaluated.
A1.2	Environmental safeguards at the data center facilities are designed, implemented, operated, and maintained, including the following: • Fire detection and suppression systems • Climate, including temperature and humidity, control systems • Uninterruptible power supplies (UPS) and backup generators • Redundant power and telecommunications lines
A1.2 (Amazon only)	• Data backup processes and procedures, along with recovery infrastructure, are designed, developed, implemented, operated, monitored and maintained to help ensure that the system is available and recoverable.

Complementary user entity controls

In designing the System, Veracode has contemplated that certain controls would be implemented by user entities to achieve the applicable trust services criteria supporting the System, which were communicated to user entities (e.g. customers) through the contract acceptance process. The complementary user entity controls presented below should not be regarded as a comprehensive list of all controls that should be employed by user entities.

- User entities who utilize the VSA and APM components are responsible for the management of their network and server infrastructure. (Criteria CC5.1; CC6.1; CC7.1; A1.1; A1.2)
- User entities are responsible for ensuring that access to the Veracode Application Security Services System is limited to authorized and appropriate individuals, including the process and controls around the administering of access and securing user IDs and passwords. (Criteria CC5.1; CC5.2)
- User entities are responsible for reviewing their employees' (including any contractors) access to the Veracode Application Security Services System and notifying Veracode of any discrepancies. (Criteria CC5.4)
- User entities of the Veracode Application Security Services System are responsible for reviewing documentation provided by Veracode related to changes to the Veracode Application Security Services System. (Criteria CC2.6)
- User entities of the Veracode Application Security Services System are responsible for reporting any security or confidentiality breaches and availability incidents, which impact the system. (Criteria CC6.2)
- User entities are responsible for approving and validating the appropriateness (and maintaining the confidentiality) of data provided to Veracode and any changes to that data. (Criteria C1.2)
- User entities are responsible for adequately securing data contained in any output reports provided by Veracode, including appropriateness of individuals accessing the output reports through the Veracode Application Security Services System and storage/disposal of the output reports. (Criteria C1.3)
- User entities are responsible for communicating security and confidentiality provisions to individuals accessing information within the Veracode Application Security Services System. (Criteria CC2.2)
- User entities are responsible for communicating any identified security violations to Veracode on a timely basis, as necessary. (Criteria CC6.2)
- User entities are responsible for communicating any changes to data retention and disposal requirements to Veracode on a timely basis. (Criteria C1.7; C1.8)
- User entities are responsible for retaining and disposing of vulnerability reports in accordance with their data retention and disposal policies. (Criteria C1.7; C1.8)

Securing the Software That Runs the World

APPLICATION SECURITY SOLUTIONS

Applications are strategic engines for business innovation – and a top target for cyber-criminals. But now you have an ally as big as your challenges. With Veracode's scalable cloud-based service and programmatic approach, you can finally secure your entire global application infrastructure – and continuously innovate without sacrificing security along the way.

CA Veracode delivers the most widely used cloud-based platform for securing web, mobile, legacy and third-party enterprise applications. By identifying critical application-layer threats before cyber-attackers can find and exploit them, Veracode helps enterprises deliver innovation to market faster – without sacrificing security.

With its combination of automation, process and speed, CA 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 are able to fully realize the advantages of DevOps environments while ensuring secure code is synonymous with high-quality code.

CA Veracode serves more than 1,400 customers worldwide across a wide range of industries. The CA Veracode Platform has assessed more than 2 trillion lines of code and helped companies fix more than 27 million security flaws.

Learn more at www.Veracode.com, on the CA Veracode blog and on Twitter.

CA Veracode Headquarters

65 Network Drive
Burlington, MA 01803
Phone: 339.674.2500
FAX: 339.674.2502
Email: contact@veracode.com

EMEA Headquarters

4th Floor, One Kingdom Street
Paddington Central
London, W2 6BD
United Kingdom
Phone: +44 (0) 203-427-6025
Email: emea@veracode.com