VERACODE

Service Organization Control 3 Report

Veracode Application Security Services System

Description relevant to Security, Availability and Confidentiality for the period April 1, 2018 to March 31, 2019

Table of Contents

SECTION 1

Assertion of Veracode

May 9, 2019

We have prepared the accompanying description of Veracode's Application Security Services System for the period April 1, 2018 to March 31, 2019 (description) based on the criteria for a description of a service organization's system set forth in DC 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria). The description is intended to provide report users with information about the Veracode Application Security Services System that may be useful when assessing the risks arising from interactions with Veracode's system, particularly information about system controls that Veracode has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Veracode uses subservice organizations Sungard Availability Services (Sungard) to provide data center hosting services, which includes physical security and environmental safeguards and Amazon Web Services (AWS) to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Veracode, to achieve Veracode's service commitments and system requirements based on the applicable trust services criteria. The description presents Veracode's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Veracode's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Veracode, to achieve Veracode's service commitments and system requirements based on the applicable trust services criteria. The description presents the service organization's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of the service organization's controls.

We confirm, to the best of our knowledge and belief, that—

1) The description presents Veracode's Application Security Services System that was designed and implemented throughout the period April 1, 2018 to March 31, 2019 in accordance with the description criteria.

2) The controls stated in the description were suitably designed throughout the period April 1, 2018 to March 31, 2019 to provide reasonable assurance that Veracode's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Veracode's controls throughout that period.

3) The controls stated in the description operated effectively throughout the period April 1, 2018 to March 31, 2019 to provide reasonable assurance that Veracode's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Veracode's controls operated effectively throughout that period.

The Management of Veracode Incorporated

SECTION 2

Independent Service Auditors' Report

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 Management of Veracode Incorporated

Approach:

We have examined management's assertion that Veracode Incorporated (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, 2018 to March 31, 2019 based on the criteria for security, availability and confidentiality in the American Institute of Certified Public Accountants' TSP Section 100, *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.

Braintree, Massachusetts
May 31, 2019

SECTION 3

Description of Veracode Application Security Services System

Relevant to Security, Availability and Confidentiality for the period April 1, 2018 to March 31, 2019

Overview of Veracode Incorporated

Veracode is a leader in helping organizations secure the software that powers their world. Veracode's SaaS platform and integrated solutions help security teams and software developers find and fix security-related defects at all points in the software development lifecycle, before they can be exploited by hackers. Our complete set of offerings help customers reduce the risk of data breaches, increase the speed of secure software delivery, meet compliance requirements, and cost effectively secure their software assets - whether that's software they make, buy or sell.

Veracode serves more than 2,000 customers across a wide range of industries, including nearly one-third of the Fortune 100 and more than 20 of Forbes' 100 Most Valuable Brands.

Over the course of this audit period Veracode underwent a number of corporate changes. The audit period (April 2018) began with Veracode as a business unit with CA Technologies. Shortly after in May 2018 CA Veracode acquired SourceClear, a software composition analysis company. Throughout the audit period Veracode continued the integration of both Source Clear's products and their Corporate assets. In November of 2018 Broadcom completed the acquisition of CA Technologies including Veracode and SourceClear. Finally, in January of 2019 Veracode became an independent company wholly owned by Thoma Bravo.

The aforementioned changes prevented some controls from being validated in their entirety as access to systems/documentation was terminated prior to audit. Compounding the lack of available systems, many employees whom were responsible for corporate systems such as procurement, finance, HR, etc. were laid off as a part of the Broadcom acquisition.

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. 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 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

Veracode Static Analysis
Veracode Static Analysis enables you to quickly identify and remediate application security flaws at scale and with efficiency. Our SaaS-based platform integrates with your development and security tools, making security testing a seamless part of your development process. Once flaws are identified, leverage in-line remediation advice and one-to-one coaching to reduce your mean time to resolve. Veracode Static Analysis is the competitive advantage you need to securely bring your applications to market at the speed of DevOps.

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.

Veracode Dynamic Analysis

Veracode Dynamic Analysis gives you a unified Dynamic Application Security Testing (DAST) solution that combines depth of coverage with unmatched scalability, scanning speed, and accuracy. The built-in automation and ease-of-use features help you quickly set up and configure single or recurring scans that run when it works best for your organization. In addition, Veracode Dynamic Analysis delivers vulnerability results with a less-than 1 percent false-positive rate, ensuring that your teams are not wasting time sorting through results and are instead able to remediate your vulnerabilities as soon as they receive their reports.

Veracode DynamicDS

Veracode DynamicDS 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.

Veracode DynamicDS 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 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.

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.

Veracode DynamicMP

Veracode DynamicMP 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.

Veracode Discovery

Veracode 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.

Veracode Software Composition Analysis

Veracode Software Composition Analysis (SCA), which includes Veracode's SourceClear offering, identifies risks from open source libraries early so you can reduce unplanned work, covering both security and license risk. SCA helps engineering keep roadmaps on track, Security achieve regulatory compliance, and the Business make smart decisions.

Veracode SCA protects your applications from open source risk by identifying known vulnerabilities in open source libraries used by your applications. In addition to providing a list of vulnerabilities when your application is scanned, Veracode SCA can also alert you when new vulnerabilities are discovered after your application has been scanned or when existing known vulnerabilities have had their severity level upgraded. Integrated with CI systems, you can fail your build based on vulnerabilities discovered as well as any components that your security team has blacklisted. As part of the Veracode Platform, Veracode SCA provides a unified experience to display all of your security testing results in one place. Additionally, the platform provides unified management of users, policies, mitigations, and integrations.

Veracode 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.

Veracode Greenlight

Deliver applications faster and meet your development timelines by writing secure code, the first time. Veracode Greenlight, an IDE or CI integrated continuous flaw feedback and secure coding education solution, returns scans in seconds, helping you answer the question “is my code secure?” Maintain your development velocity, reduce the number of flaws introduced into your application, and increase your use of secure coding practices – all with the help of Veracode Greenlight.

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.

Veracode Application Security Consulting

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.

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

Veracode Security 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.

Veracode Manual 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.

Veracode Verified

Prove your company's secure software development practices with Veracode Verified. Implementing this program helps you make security part of your competitive advantage, easily defend your AppSec budget, and better integrate security with development.

Unlike a single security attestation – we verify the secure development process around an application. With developers releasing applications and new features more frequently, a single point in time snapshot is not good enough. Instead, we focus on continuous AppSec integrated into development – that's DevSecOps.

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:

Production Systems	Platforms
Application Servers	JBoss
Web Servers	Tomcat Apache
Production Databases	Oracle, Microsoft SQL Server MySQL
Operating Systems	Solaris Windows CentOS Redhat Linux

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 within a customer's environment. 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:

Production Systems	Platforms
Production Hardware	Dell HP Thinkmate
Firewalls & Switches	Palo Alto Checkpoint Cisco

Certain technology infrastructure components relied upon to support activities 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 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.
- 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 data centers. 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. Customer information currently maintained by the Veracode Application Security Services System includes:

Data Used and Supported by the Veracode Application Security Services System		
Data Description	Data Retention	Classification
Account and user information	Life of the contract with Customer	Confidential
Application metadata	Unlimited	Confidential
Application binary files	60 days	Confidential
Application vulnerability result data	Life of the Contract with Customer	Confidential
System and application log data	6 months	Confidential

On a daily basis, a job runs 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.

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 a specialized third-party vendor 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
CC6.3 (Amazon Only)	Access to data, software, functions, and other IT resources is limited to authorized and appropriate personnel.
CC6.4	Physical access to the data center facilities is restricted to appropriate personnel who require such access to perform their job functions.
	Physical access to the data center is restricted to authorized employees and contractors using card readers and other systems (biometric scanners).
	Visitors to the data center are required to sign a visitor log.
	Administrative access to the card system and other systems (e.g. biometric readers) is limited to authorized and appropriate sub-service personnel.
	Camera surveillance of the data center is monitored and retained for a period of 90 days.
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.

CC1.0 Common Criteria Related to Control Environment

Complementary User Entity Controls	Associated Criteria
None	

CC2.0 Common Criteria Related to Communication and Information

Complementary User Entity Controls	Associated Criteria
User entities are responsible for communicating any identified security violations to Veracode on a timely basis, as necessary.	CC2.2, CC2.3
User entities are responsible for communicating security and confidentiality provisions to individuals accessing information within the Veracode Application Security Services System.	CC2.2
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.	CC2.2

CC3.0 Common Criteria Related to Risk Assessment

Complementary User Entity Controls	Associated Criteria
None	

CC4.0 Common Criteria Related to Monitoring Activities

Complementary User Entity Controls	Associated Criteria
User entities are responsible for monitoring Veracode Application Security Services System for notification and status information.	CC4.1

CC5.0 Common Criteria Related to Control Activities

Complementary User Entity Controls	Associated Criteria
None	

CC6.0 Common Criteria Related to Logical and Physical Access

Complementary User Entity Controls	Associated Criteria
User entities who utilize the VSA and APM components are responsible for the management of their network and server infrastructure.	CC6.1
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.	CC6.1, CC6.2
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.	CC6.3

CC7.0 Common Criteria Related to System Operations

Complementary User Entity Controls	Associated Criteria
User entities who utilize the VSA and APM components are responsible for the management of their network and server infrastructure.	CC7.2
User entities are responsible for communicating any identified security violations to Veracode on a timely basis, as necessary	CC7.3
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.	CC7.3

CC8.0 Common Criteria Related to Change Management

Complementary User Entity Controls	Associated Criteria
User entities who utilize the VSA and APM components are responsible for the management of their network and server infrastructure.	CC8.1

CC9.0 Common Criteria Related to Risk Mitigation

Complementary User Entity Controls	Associated Criteria
None	

A1.0 Additional Criteria for Availability

Complementary User Entity Controls	Associated Criteria
User entities who utilize the VSA and APM components are responsible for the management of their network and server infrastructure.	A1.1

C1.0 Additional Criteria for Confidentiality

Complementary User Entity Controls	Associated Criteria
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.	C1.1,
User entities are responsible for communicating any changes to data retention and disposal requirements to Veracode on a timely basis	C1.1, 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.	C1.2
User entities are responsible for retaining and disposing of vulnerability reports in accordance with their data retention and disposal policies.	C1.1, C1.2

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.

Veracode delivers the most widely used cloud-based platform for securing web, mobile, legacy and third-party enterprise applications. By identifying critical application-layer threads 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 process. As a result, enterprises are able to fully realize the advantages of DevOps environment while ensuring secure code is synonymous with high-quality code.

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

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

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

Phone +44 (0) 203 427 6025
Email emeat@veracode.com

VERACODE