VERACODE

Service Organization Control 3 Report

Veracode Application Security Services System

Description relevant to Security, Availability and Confidentiality for the period April 1, 2019 to March 31, 2020

SECTION 1

Independent Service Auditors' Report

A Division of O'Connor & Drew, P.C.
25 Braintree Hill Office Park, Suite 102, Braintree, MA 02184
Phone: (844) OCD-TECH • https://www.ocd-tech.com

Independent Service Auditors' Report.

To: The Management of Veracode Incorporated

Scope:

We have examined Veracode's accompanying assertion titled Assertion of Veracode Management (assertion) that the controls within Veracode's Application Security Services System (System) were effective throughout the period April 1, 2019 to March 31, 2020, to provide reasonable assurance that Veracode's principle service commitments and System requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Veracode utilizes Sungard Availability Services (terminated June 2019), Markley, CoreSite, and Amazon Web Services (AWS) (subservice organizations) to provide data center hosting (Markley and Sungard / CoreSite) and cloud-hosting (AWS) services. The Description of the Boundaries of the System (Section 3) indicates that Veracode's controls can provide reasonable assurance that certain service commitments and system requirements, based on the applicable trust services criteria, can be achieved only if AWS, Markley's, and CoreSite's / Sungard's controls, assumed in the design of Veracode's controls, are suitably designed and operating effectively along with related controls at the service organization. The Description presents Veracode's System and types of controls that the service organization assumes have been implemented, suitably designed, and operating effectively at AWS, Markley, and CoreSite's / Sungard's. Our examination did not extend to the services provided by AWS, Markley, and CoreSite / Sungard and we did not evaluate whether the controls management assumes have been implemented at AWS, Markley, and CoreSite / Sungard have been implemented or whether such controls were suitably designed and operating effectively throughout the period April 1, 2019 to March 31, 2020.

Service Organization's Responsibilities

Veracode is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the System to provide reasonable assurance that Veracode's service commitments and system requirements were achieved. Veracode has also provided the accompanying assertion about effectiveness of controls within the system. When preparing its assertion, Veracode is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the System.

Service Auditors' Responsibilities

Our responsibility is to express an opinion based on our examination, on whether management's assertion that controls within the System were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. 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. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination included:

- Obtaining an understanding of the System and the service organization's service commitments and system requirements;
- Assessing the risks that controls were not effective to achieve Veracode's service commitments and system requirements based on the applicable trust services criteria; and

A Division of O'Connor & Drew, P.C.
25 Braintree Hill Office Park, Suite 102, Braintree, MA 02184
Phone: (844) OCD-TECH • https://www.ocd-tech.com

- Performing procedures to obtain evidence about whether controls stated within the System were effective to achieve Veracode's service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is 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 that the controls within Veracode's Application Security Services System were effective throughout the period April 1, 2019 to March 31, 2020 to provide reasonable assurance that Veracode's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if the subservice organizations applied the controls assumed in the design of Veracode's controls through out the period April 1, 2020 to March 31, 2020.

O'Connor + Drew, P.C.

Braintree, Massachusetts
June 30, 2020

SECTION 2

Assertion of Veracode Management

VERACODE

Assertion of Veracode Management

We are responsible for designing, implementing, operating, and maintaining effective controls within Veracode's Application Security Services System (System) throughout the period April 1, 2019 to March 31, 2020, to provide reasonable assurance that Veracode's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the System is presented below and identifies the aspects of the System covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period April 1, 2019 to March 31, 2020, to provide reasonable assurance that Veracode's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Veracode's objectives for the System in applying the applicable trust services criteria are embodied in the service commitments and system requirements relevant to the applicable trust service criteria. The principle service commitments and system requirements related to the applicable trust service criteria are presented below, in Section 3.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization must achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

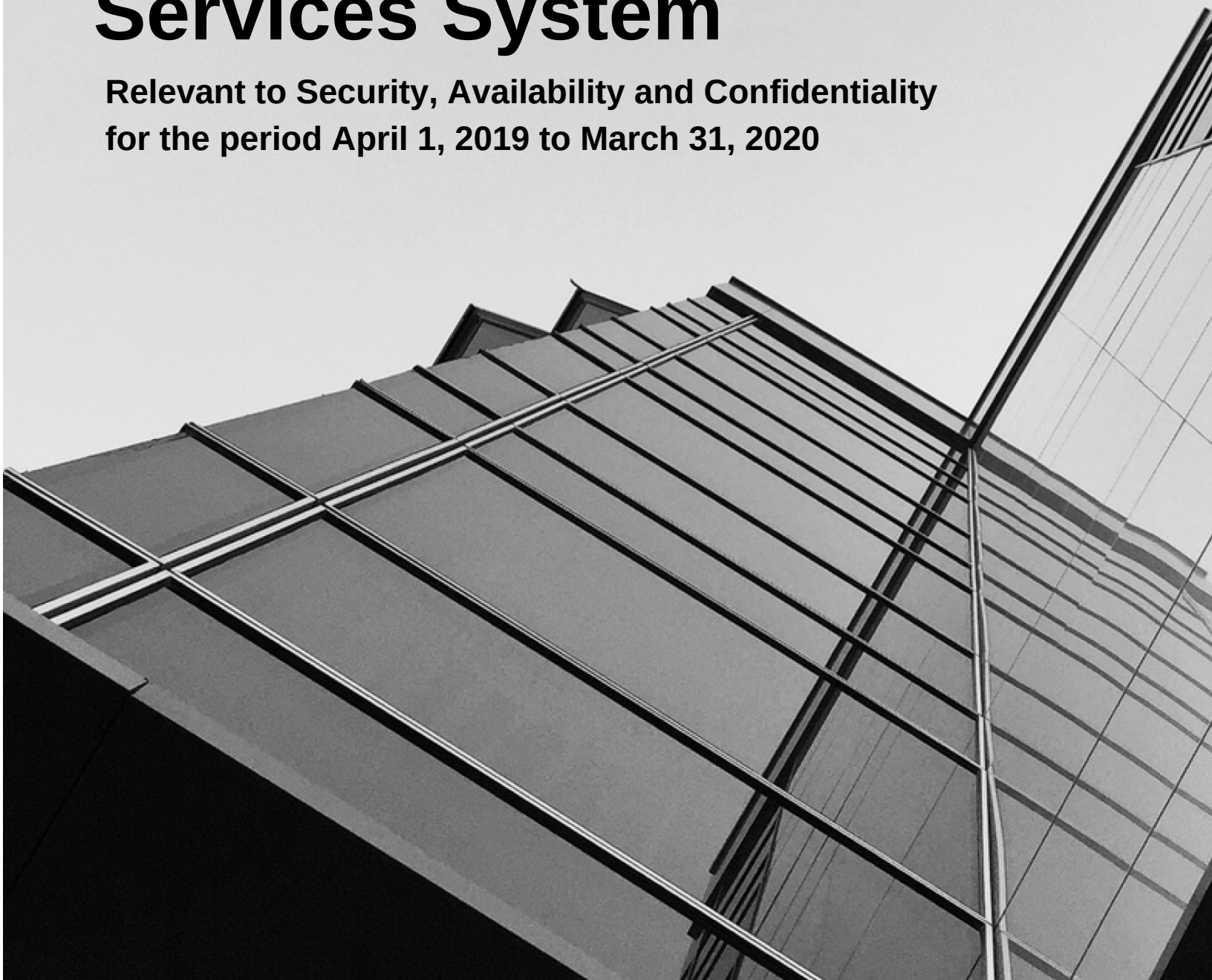
We assert that the controls within the System were affective throughout the period April 1, 2019 to March 31, 2020, to provide reasonable assurance that Veracode's service commitments and system requirements were achieved based on the applicable trust services criteria.

The Management of Veracode Incorporated

SECTION 3

Veracode's Description of the Boundaries of its Application Security Services System

Relevant to Security, Availability and Confidentiality for the period April 1, 2019 to March 31, 2020



VERACODE

Overview of Veracode Incorporated

Veracode is the leading AppSec partner for creating secure software, reducing the risk of security breach, and increasing security and development teams' productivity. As a result, companies using Veracode can move their business, and the world, forward. With its combination of automation, integrations, process, and speed, Veracode helps companies get accurate and reliable results to focus their efforts on fixing, not just finding, potential vulnerabilities.

Veracode serves more than 2,500 customers worldwide across a wide range of industries. The Veracode solution has assessed more than 14 trillion lines of code and helped companies fix more than 48 million security flaws*. Over the course of this audit period, Veracode continued to undergo a number of internal process changes due to its divestiture in January 2019 from CA/Broadcom requiring Veracode to reestablish its financial, and human resources systems. In addition, Veracode's co-location data center provider, Sungard, declared bankruptcy and exited the local market requiring Veracode to relocate to co-location data center provider CoreSite.

*This data is valid as of December 31, 2019

Veracode Application Security Services System

The Veracode Application Security Services System is designed to assist organizations in verifying an application's security state and 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, resides on Veracode's private cloud and 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 and 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 allows 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 to 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 provides fast, automated security feedback to developers with an IDE Scan (formerly Veracode Greenlight), a Pipeline Scan (formerly the DevOps Scan), and a full Policy Scan (Formerly Developers Sandbox and Policy Scan) before deployment to ensure compliance with industry standards and regulations. It gives clear guidance on what issues to focus on and how to fix them faster. Results have high accuracy without manual tuning based on 10 trillion lines of code scanned through our SaaS-based engines. Veracode's DevSecOps programs help organizations automate security feedback, align with development to reduce the security debt, and help scale to more applications through best practices and on-demand expertise.

Veracode Dynamic Analysis
Veracode Dynamic Analysis helps companies scan their web applications for exploitable vulnerabilities at scale. With an ability to test thousands of applications simultaneously and a less than 1% false positive rate coupled with comprehensive remediation guidance, customers are able to rapidly reduce their risk of a breach across their web applications. The solution integrates with Veracode Discovery, which maps your web attack surface, to scan inventoried sites.

VERACODE

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 Developer Training
Veracode Developer Training was created to help foster a higher level of security awareness and proficiency among developers with comprehensive training delivered via Veracode's 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.

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 address 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 to 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	VOSP
Application Servers	JBoss
Web Servers	Tomcat Apache
Production Databases	Oracle, Microsoft SQL Server MySQL
Operating Systems	Solaris 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, CoreSite, 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 CoreSite and Amazon Web Services, including physical security, logical security and change management.

The production hardware supporting the Veracode Application Security Services System, the part which is hosted in CoreSite, includes equipment from the following vendors:

Production Systems	VOSP
Production Hardware	Dell HP Thinkmate
Firewalls & Switches	Palo Alto Networks Check Point Software Cisco

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

Veracode's end user devices include Microsoft Windows and Apple MAC IOS computers deployed with full disk encryption. Mobile devices used by Veracode employees / contractors are required to have mobile device management software incorporated to secure data.

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 the 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
- Incident Response
- Change management, including release to production processes

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	Based on customer contract	Confidential
Application metadata	Unlimited	Confidential
Application binary files	60 days	Confidential
Application vulnerability result data	Based on customer contract	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 by a third-party vendor.

Sub-Service Organizations

Veracode utilizes Sungard Availability Services (terminated June 2019), Markley, CoreSite, and Amazon Web Services (AWS) (sub-service organizations) to provide data center hosting (Markley and Sungard / CoreSite) and cloud-hosting (Amazon) services, including physical security and environmental safeguards, to support the Veracode environment.

Securing the Software that Runs the World.

Veracode is the leading AppSec partner for confidently and efficiently creating secure software that moves your business, and the world, forward.

Veracode empowers its customers to confidently develop software by reducing the risk of security breach through comprehensive analysis, developer enablement, and governance tools.

Our passion is providing an uncompromising commitment to making secure software your competitive advantage.

Together, we can confidently respond to change faster, confidently identify and address security flaws more quickly, and we give our customers the confidence to focus on work that creates the blueprint for the future.

With a combination of automation, integrations, process, and speed, Veracode helps companies get accurate and reliable results with fewer false positives so they can be confident in knowing their software is protected by the industry's best solution.

Veracode serves more than 2,500 customers worldwide across a wide range of industries. The Veracode Solution has assessed more than 14 trillion lines of code and helped companies fix more than 48 million security flaws*.

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

*This data is valid as of December 31, 2019

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