**Service Description**

**HCL AppScan on Cloud**

This Service Description (“Service Description”) describes the HCL AppScan on Cloud service (“HCL AppScan on Cloud” or “Cloud Service”). Additional terms governing the HCL AppScan on Cloud is set forth in the HCL Cloud Service Agreement (“CSA”), available at <https://www.hcltechsw.com/wps/portal/resources/master-agreements>. This Service Description, any applicable Attachments, Orders, and the CSA are the complete agreement regarding transactions under the CSA (collectively, the "Agreement"). Any capitalized terms used but not defined in this Service Description shall have the meanings given to such terms in the CSA or other applicable documents of the Agreement.

**1. HCL AppScan on Cloud**

HCL AppScan on Cloud provides a single place to assist Customer in identifying security vulnerabilities (such as SQL Injection, Cross-Site Scripting, and Data Leakage) for a variety of applications. The service includes various types of application security scanning techniques, each of which identifies security issues in that application.

HCL AppScan on Cloud provides the following capabilities:

* Scanning Mobile Applications for security vulnerabilities.
* Scanning production or pre-production, publicly facing or on private network, Websites and Web services for security vulnerabilities using Dynamic Analysis Security Testing.
* Scanning the code within Web and Desktop applications for security vulnerabilities using Static Analysis Security Testing.
* Analyzing Web applications and Web services while they are being executed to detect security vulnerabilities using Interactive Application Security Testing.
* Identifying vulnerable Open Source packages used in an application using Software Composition Analysis.
* Detailed security vulnerability reports that include both high-level summaries of the findings and remediation steps that can be followed by developers.
* Integration with various DevOps platforms.

**1.1 Offerings**

Customer may select from the following available offerings:

**1.1.1 HCL AppScan Analyzer**

HCL AppScan Analyzer can be ordered per Application Instance, per Job (scan), per Concurrent Event (scan), or as a Concurrency Instance and allows the following types of scanning:

* Dynamic Analyzer – Test pre-production or production Websites
* Mobile Analyzer – Test iOS or Android applications
* Static Analyzer – Test byte or source code of the application

**1.1.2 HCL AppScan IAST Analyzer**

HCL AppScan IAST Analyzer identifies security vulnerabilities in running Web applications and Web services. An IAST agent instruments the application to passively monitor its behavior while it is being interacted with and report the identified vulnerabilities to HCL AppScan on Cloud. HCL AppScan IAST Analyzer can be ordered per Application Instance or per Concurrent Event (scan).

**1.1.3 HCL AppScan Open Source Analyzer**

HCL AppScan Open Source Analyzer discovers and identifies open source packages used in application code. It reviews these packages for vulnerabilities and provides remediation advice. HCL AppScan Open Source Analyzer can be ordered per Application Instance, per Concurrent Event (scan) or as a Concurrency Instance.

**2. Charge Metrics**

The following charge metrics apply to this Cloud Service:

* **Application Instance** is a copy of a uniquely named software application program connected to or managed by the Cloud Service. An Application in multiple environments (such as test, development, staging or production) or multiple instances of an Application within a single environment are considered separate Application Instances.

For this Cloud Service, Application Instances are consecutive scans of a single application further defined as follows:

* For Dynamic Testing: a Website or Web service addressable via public or private URL. Each application Instance entitles a site of up to 5,000 pages in a single domain.
* For Static Testing: a unit of code built for a single executable environment. Each Application Instance entitles scanning units of code up to 1,000,000 lines.
* For Mobile Testing: a unit of binary code that can be executed on a mobile device. Each different mobile platform (e.g., iOS and Android) constitute different application instances.
* For Open Source Testing: a unit of code built for a single executable environment. Each Application Instance entitles scanning units of code up to 1,000,000 lines.
* For Interactive Testing: a Website or Web service addressable via public or private URL.
* **Concurrent Events** is the total number of simultaneous occurrences of a specific event that is processed by or related to the use of the Cloud Service.
* **Concurrency Instance** is each access to specific configuration of the Cloud Service. For each Concurrency Instance entitlement, there is no limit on the number of Jobs performed or Application Instances (Applications connected), provided, however, that the number of Concurrent Events at any given time may not exceed the number of total concurrent entitlements for the Concurrency Instance.
* **Job** is an object within the Cloud Service that cannot be further divided and represents a computing process including all its sub-processes managed or processed by the Cloud Service. Sufficient entitlements must be obtained to cover the total number of Jobs which are processed or managed by the Cloud Service during the measurement period specified in the Order or other applicable Attachment.

|  |  |
| --- | --- |
| **AppScan per Scan** | |
| Subscription Type | Description |
| ASoC\_PerScan | Provides a single scan (which shall be considered a Job) of an application using any of these scanning technologies (Static Analyzer, Dynamic Analyzer, or Mobile Analyzer).  Purchased scans must be utilized within twelve (12) months from the purchase date, after which time they expire without refund. No time limit per scan; scans will run to completion.  Limit to only three (3) running jobs at a time. |
| **AppScan per Application** | |
| Subscription Type | Description |
| ASoC\_PerApplication | Annual subscription providing unlimited scanning of an application (“Application Instance”) using any of these scanning technologies (Static Analyzer, Dynamic Analyzer, or Mobile Analyzer) which are appropriate based on the application.  Limit to only one (1) running job at a time. |
| **AppScan Unlimited Pricing Options** | |
| Subscription Type | Description |
| AsoC\_PerConcurrent | Annual subscription providing scanning of any application using any of these scanning technologies (Static Analyzer, Dynamic Analyzer, or Mobile Analyzer).  Limit to one (1) running job for each concurrent scan entitlement.  (Concurrency Instance of “1”) |
| ASoC Premium | Annual subscription providing up to ten (10) concurrent scans of any application using any of these scanning technologies (Static Analyzer, Dynamic Analyzer, or Mobile Analyzer).  Limit up to ten (10) running jobs for each “Premium” entitlement.  (Concurrency Instance of “10”) |
| ASoC\_PerConcurrent(s), and ASoC\_Premium(s) may be combined to meet concurrency requirements that a customer may have. | |
| **AppScan IAST Analyzer Per Application** | |
| Subscription Type | Description |
| ASoC\_IAST\_PerApplication | Annual subscription providing unlimited IAST scanning of one (1) application (“Application Instance”).  Limit to only one (1) running IAST job at a time. |
| **AppScan IAST Analyzer Unlimited Pricing Options** | |
| Subscription Type | Description |
| ASoC\_IAST\_PerConcurrent | Annual subscription providing IAST scanning of any application.  Limit to one (1) running IAST job for each concurrent scan entitlement.  (Concurrency Instance of “1”) |
|  |  |
| **AppScan Open Source Analyzer Per Application** | |
| Subscription Type | Description |
| ASoC\_OSA\_PerApplication | Annual subscription providing unlimited Open Source scanning of one (1) application (“Application Instance”).  Limit to only one (1) running job at a time. |
| **AppScan Open Source Analyzer Unlimited Pricing Options** | |
| Subscription Type | Description |
| ASoC\_OSA\_PerConcurrent | Annual subscription providing Open Source scanning of any application.  Limit to one (1) running job for each concurrent scan entitlement.  (Concurrency Instance of “1”) |
| ASoC\_OSA\_Premium | Annual subscription providing up to ten (10) concurrent Open Source scans of any application.  Limit up to ten (10) running jobs for each “Premium” entitlement.  (Concurrency Instance of “10”) |
|  | |

**3. Charges and Billing**

The amount payable for the HCL AppScan on Cloud is specified in an Order.

**3.1 Partial Month Charges**

A partial month charge as specified in the Order may be assessed on a pro-rated basis.

**3.2 Billing Frequency**

Based on selected billing frequency, HCL will invoice Customer the charges due at the beginning of the billing frequency term, except for overage and usage type of charges which will be invoiced in arrears.

**3.3 Derived Benefit Locations**

Where applicable, taxes are based upon the location(s) Customer identifies as receiving benefit of the Cloud Service. HCL will apply taxes based upon the business address listed when ordering Cloud Service as the primary benefit location unless Customer provides additional information to HCL. Customer is responsible for keeping such information current and providing any changes to HCL.

**3.4 Verification**

Customer will i) maintain, and provide upon request, records, and system tools output, as reasonably necessary for HCL and its independent auditor to verify Customer's compliance with the Agreement, and ii) promptly order and pay for required entitlements at HCL's then current rates and for other charges and liabilities determined as a result of such verification, as HCL specifies in an invoice. These compliance verification obligations remain in effect during the term of the Cloud Service and for two years thereafter.

**4. Term and Renewal Options**

The term of the Cloud Service begins on the date HCL notifies Customer of their access to the Cloud Service, as documented in the Entitlement. The Entitlement will specify whether the Cloud Service renews automatically, or terminates at the end of the term.

For automatic renewal, unless Customer provides written notice not to renew at least 30 days prior to the term expiration date, the Cloud Service will automatically renew for the term specified in the Entitlement.

**5. Technical Support**

During the Subscription Period and after HCL notifies Customer that access to the Cloud Service is available, technical support information is available at the then current HCL Website made available to Customer by HCL or as set forth in the Agreement.

|  |  |  |  |
| --- | --- | --- | --- |
| **Severity** | **Severity Definition** | **Response Time Objectives** | **Response Time Coverage** |
| 1 | Critical business impact/service down: Business critical functionality is inoperable or critical interface has failed. This usually applies to a production environment and indicates an inability to access services resulting in a critical impact on operations. This condition requires an immediate solution. | Within 1 hour | 24/7 |
| 2 | Significant business impact: A service business feature or function of the service is severely restricted in its use or Customer is in jeopardy of missing business deadlines. | Within 2 business hours | M-F business hours |
| 3 | Minor business impact: Indicates the service or functionality is usable and it is not a critical impact on operations. | Within 4 business hours | M-F business hours |
| 4 | Minimal business impact: An inquiry or non-technical request. | Within 1 business day | M-F business hours |

**5.1 Access to Customer Data**

HCL will be able to access Customer data for the purpose of diagnosing issues with the service, and facilitating scans of Customer’s application by the service. HCL will access the data only for the purposes of fixing defects or to provide support for HCL products or services.

**6. Service Level Agreement**

HCL provides the following availability service level agreement ("SLA") for the Cloud Service. The SLA is not a warranty and is Customer’s sole and exclusive remedy. The SLA is available only to Customer and applies only to use in production environments.

**6.1 Availability Credits**

Customer must log a Severity 1 support ticket with the HCL technical support help desk within 24 hours of first becoming aware that there is a critical business impact and the Cloud Service is not available. Customer must reasonably assist HCL with any problem diagnosis and resolution.

A support ticket claim for failure to meet an SLA must be submitted within 3 business days after the end of the contracted month. Compensation for a valid SLA claim will be a credit against a future invoice for the Cloud Service based on the duration of time during which production system processing for the Cloud Service is not available ("Downtime"). Downtime is measured from the time Customer reports the event until the time the Cloud Service is restored and does not include time related to a scheduled or announced maintenance outage; causes beyond HCL's control; problems with Customer or third party content or technology, designs or instructions; unsupported system configurations and platforms or other Customer errors; or Customer-caused security incident or Customer security testing. HCL will apply the highest applicable compensation based on the cumulative availability of the Cloud Service during each contracted month, as shown in the table below. The total compensation with respect to any contracted month cannot exceed 10 percent of one twelfth (1/12th) of the annual charge for the Cloud Service.

**6.2 Service Levels**

Availability of the Cloud Service during a contracted month

|  |  |
| --- | --- |
| **Availability during a contracted month** | **Compensation (% of monthly subscription fee\* for contracted month that is the subject of a claim)** |
| Less than 99.9% | 2% |
| Less than 99% | 5% |
| Less than 95% | 10% |

\* If the Cloud Service was acquired from an HCL Business Partner, the monthly subscription fee will be calculated on the then-current list price for the Cloud Service in effect for the contracted month which is the subject of a claim, discounted at a rate of 50%. HCL will make a rebate directly available to Customer. Availability, expressed as a percentage, is calculated as: the total number of minutes in a contracted month minus the total number of minutes of Downtime in a contracted month divided by the total number of minutes in the contracted month.

**7. Technology Preview Code**

Technology Preview Code (TPC) may be included or distributed with the Program or updates to it but are not part of the Program. TPC is licensed under the same terms as the Program, except as provided below. TPC will be identified as such in the Notices File (or in an updated Notices File accompanying the updates). Some or all of the TPC may not be made generally available by HCL as or in a product. Licensee is permitted to use TPC only for internal use for evaluation purposes. REGARDLESS OF OTHER STATEMENTS MADE AT OR BEFORE THE TIME OF PURCHASE, IT IS LICENSEE'S RESPONSIBILITY TO DETERMINE IF THE PROGRAM IS APPROPRIATE OR SAFE FOR LICENSEE'S WEBSITE, WEB APPLICATION OR TECHNICAL ENVIRONMENT. LICENSEE ACKNOWLEDGES AND ACCEPTS ALL RISKS ASSOCIATED WITH THE USE OF THE PROGRAM. The Notices File or Proof of Concept agreement (POC) may limit this evaluation use to an evaluation period. If so, at the end of such evaluation period Licensee must cease using and uninstall the TPC. HCL provides the TPC without obligation of support and "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF TITLE, NON-INFRINGEMENT OR NON-INTERFERENCE AND ANY IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Licensee may not transfer TPC to another party except as a transfer accompanying the Program. TPC may contain a disabling device that will prevent it from being used after the evaluation period ends. Licensee will not tamper with this disabling device or the TPC. Licensee should take precautions to avoid any loss of data that might result when the TPC can no longer be used.

**8. HCL AppScan on Cloud Additional Terms**

**8.1 Security Scans**

Security scans may not identify all security risks in an application, nor are they designed or intended for use in hazardous environments requiring fail-safe operation, including without limitation aircraft navigation, air traffic control systems, weapon systems, life support systems, nuclear facilities, or any other applications in which failure to identify security risks could lead to death, personal injury, or property damage. Security scans are not warranted to operate uninterrupted or error free.

The HCL AppScan on Cloud can be used to help Customer meet compliance obligations, which may be based on laws, regulations, standards or practices. Any directions, suggested usage, or guidance provided by the Service does not constitute legal, accounting, or other professional advice, and Customer is cautioned to obtain its own legal or other expert counsel. Customer is solely responsible for ensuring that Customer and Customer’s activities, applications and systems comply with all applicable laws, regulations, standards and practices. Use of this Service does not guarantee compliance with any law, regulation, standard or practice.

The HCL AppScan on Cloud performs invasive and non-invasive tests on the Website and Web or mobile application Customer chooses to scan. Certain laws prohibit any unauthorized attempt to penetrate or access computer systems. Customer authorizes HCL to perform the Services as described herein and acknowledges that the Services constitute authorized access to Customer's computer systems. HCL may disclose this grant of authority to a third party if deemed necessary to perform the Services. The testing entails certain risks, including without limitation the following:

Customer’s computer systems while running applications under test may hang or crash, resulting in temporary system unavailability or loss of data;

* the performance and throughput of Customer’s systems, as well as the performance and throughput of associated routers and firewalls, may be temporarily degraded during testing;
* excessive amounts of log messages may be generated, resulting in excessive log file disk space consumption;
* data may be changed or deleted as a result of probing vulnerabilities;
* alarms may be triggered by intrusion detection systems;
* emails may be triggered by the email function of the Web application being tested;
* the HCL AppScan on Cloud may intercept the traffic of the monitored network for the purpose of looking for events.

Any service level agreement rights or remedies provided by HCL and relating to the Websites or applications subject to testing will be waived during any testing activity.

In the event that Customer inputs authenticated log-in credentials for the application under test into the Service, Customer should only input such credentials for test accounts and not for production users. Use of production user credentials may result in personal data being transmitted via the Service.

The HCL AppScan on Cloud may be configured to scan production Web applications. When Customer sets the scan type as "production," the service is designed to perform scans in a manner that reduces the risks listed above; however, in certain situations the HCL AppScan on Cloud may lead to performance degradation or instability within the tested production sites and infrastructure. HCL makes no warranties or representations with respect to the suitability of using the HCL AppScan on Cloud to scan production sites.

IT IS CUSTOMER’S RESPONSIBILITY TO DETERMINE IF THE SERVICE IS APPROPRIATE OR SAFE FOR CUSTOMER’S WEBSITE, WEB APPLICATION, MOBILE APPLICATION OR TECHNICAL ENVIRONMENT.

The HCL AppScan on Cloud is designed to identify a variety of potential security and compliance issues in mobile and Web applications and Web services. It does not test all vulnerabilities or compliance risks, nor does it act as a barrier to security attacks. Security threats, regulations and standards continually change, and the Service may not reflect all such changes. The security and compliance of Customer’s Web application, systems and employees, and any remedial actions, are Customer’s responsibility alone. It is solely within Customer’s discretion to use or not use any of the information provided by the Service.

Certain laws prohibit any unauthorized attempt to penetrate or access computer systems. CUSTOMER IS RESPONSIBLE FOR ENSURING THAT CUSTOMER DOES NOT USE THE SERVICE TO SCAN ANY WEBSITES AND/OR APPLICATIONS OTHER THAN WEBSITES AND/OR APPLICATIONS OWNED BY CUSTOMER OR THOSE THAT CUSTOMER HAS THE RIGHT AND AUTHORITY TO SCAN.

For the purpose of clarity, Customer Content described in the Data Protection section of the CSA is also deemed to include data that may become accessible to HCL during Application Penetration Testing.

**8.2 Data Use & Cookies**

Please review HCL Privacy Statement information here: <https://www.hcltech.com/privacy-statement>

Customer is aware and agrees that HCL may, as part of the normal operation and support of the HCL AppScan on Cloud, collect personal information from Customer (Customer’s employees and contractors) related to the use of the HCL AppScan on Cloud, through tracking and other technologies. HCL does so to gather usage statistics and information about effectiveness of the HCL AppScan on Cloud for the purpose of improving user experience and/or tailoring interactions with Customer. Customer confirms that it will obtain or have obtained consent to allow HCL to process the collected personal information for the above purpose within HCL, other HCL companies and their subcontractors, wherever HCL and such subcontractors do business, in compliance with applicable law. HCL will comply with requests from Customer’s employees and contractors to access, update, correct or delete their collected personal information.

As part of the HCL AppScan on Cloud, that includes reporting activities, HCL will prepare and maintain de-identified and aggregate information collected from HCL AppScan on Cloud (called "Security Data"). The Security Data will not identify Customer, or an individual except as provided herein. Customer herein additionally agrees that HCL may use and/or copy the Security Data only for the following purposes:

* publishing and/or distributing the Security Data (e.g., in compilations and/or analyses related to cybersecurity);
* developing or enhancing products or services;
* conducting research internally or with third parties; and
* lawful sharing of confirmed third party perpetrator information.

**8.3 Enabling Software**

The Cloud Service may require the use of enabling software that Customer downloads to Customer systems to facilitate use of the Cloud Service. Customer may use Enabling Software listed below solely in connection with use of the Cloud Service. Enabling Software is provided to Customer under following terms:

|  |  |
| --- | --- |
| **Enabling Software** | **Applicable License Terms (if any)** |
| Static Analyzer Client Utility (IRX Generator) | Provide for use AS-IS |
| AppScan GO! | Provide for use AS-IS |
| AppScan Presence | Provide for use AS-IS |
| AppScan IAST Agent | Provide for use AS-IS |