**服务描述**

**HCL AppScan on Cloud**

此服务描述（“服务描述”）对 HCL AppScan on Cloud 服务（“HCL AppScan on Cloud”或“云服务”）进行了说明。HCL 云服务协议（“CSA”）中规定了 HCL AppScan on Cloud 的其他约束条款，具体内容请访问 <https://www.hcltechsw.com/wps/portal/resources/master-agreements>。此服务描述、任何适用附件、条令和 CSA 构成了 CSA 事务相关完整协议（统称为“协议”）。此服务描述中所使用但未进行定义的任何术语名称应与 CSA 或其他适用协议文档中的同一术语涵义相同。

**1. HCL AppScan on Cloud**

HCL AppScan on Cloud 提供了一个统一位置，可帮助客户识别各种应用程序的安全漏洞（例如 SQL 注入、跨站点脚本编制和数据泄露）。该服务包含多种应用程序安全扫描技术，每种技术可用于识别特定应用程序中的安全问题。

HCL AppScan on Cloud 提供以下功能：

* 扫描移动应用程序以查找安全漏洞。
* 利用动态分析安全测试，扫描生产或生产前公共或私有网络上的 Web 站点和 Web 服务以查找安全漏洞。
* 利用静态分析安全测试，扫描 Web 和桌面应用程序内的代码以查找安全漏洞。
* 利用交互应用程序安全测试，分析正在运行的 Web 应用程序和 Web 服务以检测安全漏洞。
* 利用软件组成分析，识别应用程序中所使用的易受攻击的开放式源代码软件包。
* 详细安全漏洞报告，其中包含开发人员可遵循的结果和修复步骤的高级概要。
* 与多种 DevOps 平台集成。

**1.1 产品/服务**

客户可以选择以下可用产品/服务项目：

**1.1.1 HCL AppScan IAST Analyzer**

HCL AppScan Analyzer 可以按应用程序实例、作业（扫描）、并发事件（扫描）或并发实例进行订购，支持以下类型扫描：

* Dynamic Analyzer – 测试生产前或生产 Web 站点
* Mobile Analyzer – 测试 iOS 或 Android 应用程序
* Static Analyzer – 测试应用程序字节或源代码

**1.1.2 HCL AppScan IAST Analyzer**

HCL AppScan IAST Analyzer 可识别 Web 应用程序和 Web 服务运行期间的安全漏洞。IAST 代理程序会检测应用程序以被动监控其交互行为，并将所发现的漏洞报告给 HCL AppScan on Cloud。HCL AppScan IAST Analyzer 可以按应用程序实例或并发事件（扫描）进行订购。

**1.1.3 HCL AppScan Open Source Analyzer**

HCL AppScan Open Source Analyzer 可发现和识别应用程序代码中所使用的开放式源代码软件包。该工具会对这些软件包进行检查以查找漏洞并提供修复建议。HCL AppScan Analyzer 可以按应用程序实例、并发事件（扫描）或并发实例进行订购。

**2. 收费指标**

该云服务提供以下收费指标：

* **应用程序实例**是云服务所连接或管理的唯一名称软件应用程序的副本。多种环境（例如测试、开发、登台或生产）中某个应用程序或单一环境中某个应用程序的多个实例被视为单独的应用程序实例。

对于该云服务，应用程序实例为单个应用程序的连续扫描，进一步定义如下：

* 对于动态测试：可通过公共或私有 URL 访问的 Web 站点或 Web 服务。每个应用程序实例在单个域中最多支持 5,000 个页面的站点。
* 对于静态测试：专为单一执行环境构建的代码单元。每个应用程序实例最多支持 1,000,000 行代码单元扫描。
* 对于移动测试：可在移动设备上运行的二进制代码单元。每个不同的移动平台（例如 iOS 和 Android）构成不同的应用程序实例。
* 对于开放式源代码测试：专为单一执行环境构建的代码单元。每个应用程序实例最多支持 1,000,000 行代码单元扫描。
* 对于交互式测试：可通过公共或私有 URL 访问的 Web 站点或 Web 服务。
* **并发事件数**是指使用云服务时所处理或相关联的特定事件的同时并发总数。
* **并发实例**是指对特定云服务配置的每次访问。对于每项并发实例权利，所执行的作业数量或应用程序实例（连接的应用程序）数量没有限制，但前提条件是，任何特定时间的并发事件数量不能超过并发实例的总并发权利数量。
* **作业**是指云服务内不能再分解的对象，代表某个计算进程，包括云服务所管理或处理的所有子进程。必须获得足够的权利，才能涵盖条令或其他适用附件中规定的测量期限内云服务所处理或管理的总作业数量。

|  |  |
| --- | --- |
| **AppScan（按扫描）** | |
| 订阅类型 | 描述 |
| ASoC\_PerScan | 允许利用以下任意扫描技术（Static Analyzer、Dynamic Analyzer 或 Mobile Analyzer）单次扫描某个应用程序（应视为一项作业）。  所购买的扫描必须在十二 (12) 个月内用完（自购买日算起），否则将会过期而不予退款。每次扫描没有时间限制，扫描将一直运行到结束为止。  限制为一次仅运行三 (3) 个作业。 |
| **AppScan（按应用程序）** | |
| 订阅类型 | 描述 |
| ASoC\_PerApplication | 年度订阅，允许利用以下任意扫描技术（Static Analyzer、Dynamic Analyzer 或 Mobile Analyzer）无限次扫描某个应用程序（“应用程序实例”）。  限制为一次仅运行一 (1) 个作业。 |
| **AppScan 无限定价选项** | |
| 订阅类型 | 描述 |
| AsoC\_PerConcurrent | 年度订阅，允许利用以下任意扫描技术（Static Analyzer、Dynamic Analyzer 或 Mobile Analyzer）扫描任何应用程序。  限制为每个并发扫描权利运行一 (1) 个作业。  （“1”个并发实例） |
| ASoC Premium | 年度订阅，允许利用以下任意扫描技术（Static Analyzer、Dynamic Analyzer 或 Mobile Analyzer）对任何应用程序最多进行十 (10) 个并发扫描。  限制为每个“高级”权利最多运行十 (10) 个作业。  （“10”个并发实例） |
| ASoC\_PerConcurrent(s) 和 ASoC\_Premium(s) 可结合使用以满足客户的并发要求。 | |
| **AppScan IAST Analyzer（按应用程序）** | |
| 订阅类型 | 描述 |
| ASoC\_IAST\_PerApplication | 年度订阅，允许对一 (1) 个应用程序（“应用程序实例”）进行无限 IAST 扫描。  限制为一次仅运行一 (1) 个 IAST 作业。 |
| **AppScan IAST Analyzer 无限定价选项** | |
| 订阅类型 | 描述 |
| ASoC\_IAST\_PerConcurrent | 年度订阅，允许对任何应用程序进行 IAST 扫描。  每个并发扫描权利限制运行一 (1) 个 IAST 作业。  （“1”个并发实例） |
|  |  |
| **AppScan Open Source Analyzer（按应用程序）** | |
| 订阅类型 | 描述 |
| ASoC\_OSA\_PerApplication | 年度订阅，允许对一 (1) 个应用程序（“应用程序实例”）进行无限开放式源代码扫描。  限制为一次仅运行一 (1) 个作业。 |
| **AppScan Open Source Analyzer 无限定价选项** | |
| 订阅类型 | 描述 |
| ASoC\_OSA\_PerConcurrent | 年度订阅，允许对任何应用程序进行开放式源代码扫描。  限制为每个并发扫描权利运行一 (1) 个作业。  （“1”个并发实例） |
| ASoC\_OSA\_Premium | 年度订阅，允许对任何应用程序最多进行十 (10) 个并发开放式源代码扫描。  限制为每个“高级”权利最多运行十 (10) 个作业。  （“10”个并发实例） |
|  | |

**3. 费用和计费**

HCL AppScan on Cloud 的应付金额在订单中指定。

**3.1 每月日均费用**

订单中指定的每月日均费用可以按比例评估。

**3.2 计费周期**

根据选定的计费周期，HCL 将向客户开具在计费周期开始时应支付的费用，但超出部分和超额使用类型的费用将以欠款方式开具发票。

**3.3 衍生受益地**

在适用的情况下，将根据客户确定作为云服务受益地的地点计算税金。除非客户向 HCL 提供其他信息，否则 HCL 将把订购云服务时列出的营业地址作为主要受益地来征税。客户有责任保持更新此类信息，并向 HCL 提供任何更改。

**3.4 验证**

客户：i) 维护并应请求提供记录及系统工具输出，以便 HCL 及其独立审计师合理必要地验证客户是否遵守本协议；并 ii) 将按照 HCL 当时的价格针对所需的权利立即订购并付款，并支付 HCL 在发票中指定的由于此类验证而确定的其他费用和负债。这些合规性验证义务在云服务期限内以及此后的两年内保持有效。

**4. 期限和续订选项**

如“权利”中所述，云服务期限从 HCL 通知客户其有权访问云服务之日起开始。“权利”将指定云服务是自动续订还是在期限结束时终止。

对于自动续订，除非客户在期限到期日期前至少 30 天提供不续约书面通知，否则云服务将自动续订，续订期限为“权利”中指定的期限。

**5. 技术支持**

在订阅期内，在 HCL 通知客户可以访问云服务之后，技术支持信息可在当时由 HCL 提供给客户或协议中规定的当前 HCL Web 站点上获得。

|  |  |  |  |
| --- | --- | --- | --- |
| **严重性** | **严重性定义** | **响应时间目标** | **响应时间范围** |
| 1 | 业务影响严重/服务停止：业务关键功能无法操作或关键接口崩溃。这通常适用于生产环境，表示无法访问服务，会对运营造成严重影响。这种情况要求立即解决。 | 1 小时内 | 24/7 |
| 2 | 业务影响重大：服务业务功能或服务功能在使用过程中受到严格限制，或者客户面临错过业务截止日期的危险。 | 2 小时内（营业时间） | 周一至周五（营业时间） |
| 3 | 业务影响小：表示服务或功能可用，且对运营没有造成严重影响。 | 4 小时内（营业时间） | 周一至周五（营业时间） |
| 4 | 业务影响微乎其微：查询或非技术请求。 | 1 天内（营业日） | 周一至周五（营业时间） |

**5.1 访问客户数据**

HCL 可以访问客户数据，以诊断服务问题，并促进该服务对客户应用程序的扫描。HCL 仅出于修复缺陷或为 HCL 产品或服务提供支持的目的访问数据。

**6. 服务级别协议**

HCL 为云服务提供以下可用性服务级别协议 ("SLA")。SLA 不是保证，而是客户的唯一和专有补救措施。SLA 仅适用于客户，并且仅适用于生产环境。

**6.1 可用度扣抵**

客户必须在首次意识到对业务产生重大影响并且无法使用云服务的 24 小时内，在 HCL 技术支持帮助台上记录严重级别 1 支持请求。客户必须合理协助 HCL 诊断和解决问题。

如果未能满足 SLA 要求，则必须在合同规定的月份结束后的 3 个工作日内提交支持请求。针对有效 SLA 索赔的补偿将基于无法使用云服务的生产系统进行处理的持续时间（“停机时间”），从云服务的未来发票中扣除。停机时间是指从客户报告事件到恢复云服务之间的时间，不包括与计划或宣布的维护中断有关的时间；超出 HCL 控制的原因；客户或第三方内容或技术、设计或说明存在的问题；不支持的系统配置和平台或其他客户错误；或客户引起的安全事件或客户安全测试。HCL 将根据每个合同规定的月份内云服务的累积可用性来应用最高的适用补偿，如下表所示。任何合同规定月份的总补偿不得超过云服务年度费用的十二分之一 (1/12) 的 10%。

**6.2 服务级别**

合同规定月份期间云服务的可用性

|  |  |
| --- | --- |
| **合同规定月份期间的可用性** | **补偿（合同规定月份的月订阅费（索赔标的）\*的百分比）** |
| 低于 99.9% | 2% |
| 低于 99% | 5% |
| 低于 95% | 10% |

\* 如果云服务是从 HCL 业务合作伙伴那里购买的，则每月的订阅费（索赔标的）将根据合同规定月份有效的云服务当前价格计算，折扣为 50%。HCL 将为客户直接提供折扣。可用性以百分比表示，计算方法如下：合同规定月份中的总分钟数减去合同规定月份中“停机时间”的总分钟数，然后除以合同规定月份中的总分钟数。

**7. 技术预览代码**

技术预览代码 (TPC) 可能包含在本程序或其更新中或与之一起分发，但不属于本程序。TPC 根据与本程序相同的条款获得许可，但下文规定的除外。TPC 将在通知文件中（或更新随附的更新后的通知文件中）确定。部分或全部 TPC 一般不能由 HCL 作为产品或在产品中提供。被许可方只能将 TPC 用于内部评估目的，而不能用于生产环境。无论在购买时或购买前所作的其他声明如何，被许可方有责任确定程序对于被许可方的 Web 站点、Web 应用程序或技术环境而言是否适当或安全。被许可方确认并接受与使用程序有关的所有风险。通知文件或概念证明 (POC) 协议可以将此评估使用限制在评估期内。如果是这样，则在评估期结束时，被许可方必须停止使用并卸载 TPC。HCL 按“原样”提供 TPC，不承担任何支持责任，不提供任何种类的（无论是明示还是暗示）保证，包括但不限于有关权利、非侵权、非干扰以及隐含的有关适销和适用于某种特定用途的保证和条件。

被许可方不得将 TPC 转让给另一方，除非伴随本程序转让。TPC 可能包含禁用装置，可防止其在评估期结束后继续被使用。被许可方不得篡改该禁用装置或 TPC。被许可方应采取预防措施以避免因 TPC 不能继续被使用而可能导致的任何数据损失。

**8. HCL AppScan on Cloud 附加条款**

**8.1 安全扫描**

安全扫描可能不会发现应用程序中的所有安全风险，其设计和意图也并非用于要求确保无故障运行的危险环境，这些操作包括但不限于飞机导航、空中交通管制系统、武器系统、生命支持系统、核设施或任何其他应用程序，在这些应用程序中，如果未能发现安全风险，可能导致人员死亡、人身伤害或财产损失。安全扫描无法保证不间断或无错误运行。

HCL AppScan on Cloud 可用于帮助客户基于法律、法规、标准或惯例履行合规性义务。服务提供的任何指导或建议用法均不构成法律、会计或其他专业建议，客户应谨慎地自行寻求法律或其他专家顾问的建议。客户全权负责确保客户及客户的活动、应用程序和系统符合所有适用的法律、法规、标准和惯例。使用本服务并不保证会遵守所有法律、法规、标准或惯例。

HCL AppScan on Cloud 会在客户选择进行扫描的 Web 站点、Web 或移动应用程序上执行侵入性和非侵入性测试。某些法律禁止企图在未经授权的情况下侵入或访问计算机系统。客户授权 HCL 执行本协议所述的服务，并承认这些服务包括对客户计算机系统的授权访问。HCL 可将此项授权披露给第三方，如果这样做对履行服务而言有必要。测试会带来某些风险，这些风险包括但不限于：

运行应用程序以进行测试时，客户的计算机系统可能会挂起或崩溃，从而导致系统暂时不可用或数据丢失；

* 在测试过程中，客户系统以及相关路由器和防火墙的性能和吞吐量可能会暂时降低；
* 可能会生成大量日志消息，从而导致日志文件磁盘空间大量消耗；
* 探测漏洞可能会更改或删除数据；
* 入侵检测系统可能触发警报；
* 接受测试的 Web 应用程序的电子邮件功能可能会触发电子邮件；
* HCL AppScan on Cloud 可能会为了查找事件而拦截被监视网络的流量。

在任何测试活动期间，HCL 提供的、与测试 Web 站点或应用程序相关的所有服务级别协议权利或补救措施都将予以豁免。

测试期间，当客户在服务中输入应用程序已验证的登录凭证时，客户应该仅输入此类测试帐户的凭证，而不是生产用户的凭证。使用生产用户凭证可能会导致通过该服务传输个人数据。

HCL AppScan on Cloud 可以配置为扫描生产 Web 应用程序。当客户将扫描类型设置为“生产”时，该服务将以降低上述风险的方式执行扫描；但是，在某些情况下，HCL AppScan on Cloud 可能会导致测试的生产站点和基础设施的性能下降或不稳定。对于使用 HCL AppScan on Cloud 来扫描生产站点的适用性，HCL 不作任何保证或声明。

客户有责任确定该服务对于其 Web 站点、Web 应用程序、移动应用程序或技术环境是否合适或安全。

HCL AppScan on Cloud 旨在识别移动应用程序、Web 应用程序以及 Web 服务中的各种潜在安全性与合规性问题。它不会对所有漏洞或合规性风险进行测试，也不会充当遭遇安全攻击时的屏障。安全威胁、法规和标准在不断变化，该服务可能不会反映所有这些变化。客户的 Web 应用程序、系统和员工的安全性与合规性，以及任何补救措施，都是客户自己的责任。客户可自行决定是否使用本服务提供的任何信息。

某些法律禁止企图在未经授权的情况下侵入或访问计算机系统。客户有责任确保不会使用该服务扫描除客户拥有的或客户有权进行扫描的 Web 站点和/或应用程序以外的任何 Web 站点和/或应用程序。

为清晰起见，CSA 的数据保护部分中描述的客户内容也应被视为包括 HCL 在应用程序渗透测试期间可以访问的数据。

**8.2 数据使用和 Cookie**

请在此查阅“HCL 隐私声明”：<https://www.hcltech.com/privacy-statement>

客户了解并同意，HCL 作为 HCL AppScan on Cloud 正常运行和支持的一部分，会通过跟踪和其他技术向客户（客户的员工和承包商）收集与使用 HCL AppScan on Cloud 相关的个人信息。HCL 这样做是为了收集有关 HCL AppScan on Cloud 有效性的使用统计数据和信息，以提升用户体验和/或针对客户调整交互方式。客户确认，在符合适用法律要求的情况下，客户将获得或已获得同意，以允许 HCL 在 HCL、其他 HCL 公司及其分包商（无论 HCL 和此类分包商在何处开展业务）内处理为上述目的收集的个人信息。HCL 将满足客户员工和承包商访问、更新、更正或删除其收集的个人信息的要求。

作为包括报告活动在内的 HCL AppScan on Cloud 的一部分，HCL 将编制和维护从 HCL AppScan on Cloud 收集的去识别化和汇总的信息（称为“安全数据”）。安全数据将无法识别客户或个人，但此处规定的情况除外。此外，客户还在此同意 HCL 仅可为以下目的使用和/或复制安全数据：

* 发布和/或分发安全数据（例如，针对网络安全进行汇总和/或分析）；
* 开发或强化产品或服务；
* 通过内部或第三方执行调研；以及
* 合法分享确认的第三方攻击者信息。

**8.3 支持软件**

云服务可能需要使用客户机下载到客户机系统的支持软件以方便使用云服务。客户只能在与云服务使用相关的情况下使用下列支持软件。根据以下条款向客户提供支持软件：

|  |  |
| --- | --- |
| **支持软件** | **适用的许可条款（如有）** |
| Static Analyzer Client Utility (IRX Generator) | 按原样提供以供使用 |
| AppScan GO! | 按原样提供以供使用 |
| AppScan Presence | 按原样提供以供使用 |
| AppScan IAST 代理 | 按原样提供以供使用 |