**服務說明**

**HCL AppScan on Cloud**

這項服務說明（「服務說明」）描述 HCL AppScan on Cloud 服務（「HCL AppScan on Cloud」或「雲端服務」）。其他控管 HCL AppScan on Cloud 的條款詳述於 HCL 雲端服務協議（「CSA」），可參閱此處 <https://www.hcltechsw.com/wps/portal/resources/master-agreements>。此服務說明、任何適用附件、指示與 CSA 是與根據 CSA 相關之交易的完整協議（以下統稱為「協議」）。此服務說明中使用但未經定義的大寫術語應具有 CSA 或其他適用協議文件賦予的意義。

**1. HCL AppScan on Cloud**

HCL AppScan on Cloud 提供單一空間，協助客戶識別各種應用程式的安全漏洞（例如 SQL 注入、 跨網站 Scripting 及資料洩漏）。服務包含各種應用程式安全掃描技術類型，每種技術都可以識別該應用程式內的安全問題。

HCL AppScan on Cloud 提供下列功能：

* 掃描應用程式的漏洞
* 使用動態分析安全測試，針對公共或私人網路、網站及 Web 服務，掃描正式作業或前置正式作業的安全漏洞。
* 使用靜態分析安全測試，在 Web 與桌面應用程式內掃描程式碼的安全漏洞。
* 使用互動式應用程式安全測試，在執行 Web 應用程式和 Web 服務時進行分析，以偵測安全漏洞。
* 使用軟體組合分析，識別應用程式中使用的有漏洞開放原始碼套件。
* 詳細的安全漏洞報告包含發現項目的高階摘要和開發人員可遵循的補救措施步驟。
* 與各種 DevOps 平台整合。

**1.1 供應項目**

客戶可從以下可用供應項目中進行選擇：

**1.1.1 HCL AppScan Analyzer**

HCL AppScan Analyzer 的訂購方式可按照應用程式執行個體、工作（掃描）、並行事件（掃描）或並行執行個體，且此服務允許以下的掃描類型：

* 動態分析器 – 測試前置生產作業或生產作業網站
* 行動分析器 – 測試 iOS 或 Android 應用程式
* 靜態分析器 – 測試應用程式的位元組或開放原始碼

**1.1.2 HCL AppScan IAST Analyzer**

HCL AppScan IAST Analyzer 可在執行中的 Web 應用程式與 Web 服務中識別安全漏洞。IAST 代理程式檢測應用程式，以在與應用程式互動時被動地監視其行為，並將識別的漏洞向 HCL AppScan on Cloud 回報。HCL AppScan IAST Analyzer 的訂購方式可按照應用程式執行個體或並行事件（掃描）。

**1.1.3 HCL AppScan Open Source Analyzer**

HCL AppScan Open Source Analyzer 發現與識別在應用程式程式碼所用的開放原始碼套件。其檢閱這些套件，確認是否有漏洞，並提供補救措施建議。HCL AppScan Open Source Analyzer 的訂購方式可按照應用程式執行個體、並行事件（掃描）或並行執行個體。

**2. 收費度量**

以下收費度量適用於此雲端服務：

* **應用程式實例**是連接到雲端服務，或由雲端服務管理的唯一命名軟體應用程式副本。多個環境（例如測試、開發、暫置或正式作業）中的應用程式，或單一環境中應用程式的多個實例，視為分別的應用程式實例。

針對此雲端服務，應用程式實例是對單一應用程式的連續掃描，進一步的定義如下：

* 針對動態測試：可透過公共或私人 URL 定址的網站或 Web 服務。每個應用程式實例在單一網域中可授權高達 5,000 個頁面。
* 針對靜態測試：為單一可執行環境所建置的代碼單位。每個應用程式實例可授權掃描高達 1,000,000 行代碼單位。
* 針對行動測試：可於行動裝置執行的二進位代碼單位。每種不同的行動平台（例如 iOS 及 Android）含有不同的應用程式實例。
* 開放程式碼測試：為單一可執行環境所建置的代碼單位。每個應用程式實例可授權掃描高達 1,000,000 行代碼單位。
* 針對互動式測試：可透過公共或私人 URL 定址的網站或 Web 服務。
* **並行事件**是特定事件的同時出現項目總數，該特定事件由雲端服務所處理或與雲端服務使用情形相關。
* **並行實例**是每次存取雲端服務的特定配置。針對每個並行實例授權，提供的執行工作或應用程式實例（已連接的應用程式）之數量並沒有限制，然而任何特定時間的並行事件不得超過並行實例的總並行授權數。
* **工作**是在雲端服務內的物件，代表一個不可進一步分割的計算流程，其中包括由雲端服務管理或處理的所有子處理程序。必須取得足夠的授權，在指示或其他適用附件所指定的測量期間，涵蓋雲端服務處理或管理的工作總數。

|  |  |
| --- | --- |
| **依掃描的 AppScan** | |
| 訂閱類型 | 說明 |
| ASoC\_PerScan | 使用任何這些掃描技術（Static Analyzer、Dynamic Analyzer 或 Mobile Analyzer），提供應用程式的單次掃描（應視為一項工作）。  購買的掃描務必於購買日期起十二 (12) 個月內使用，期限過後將會逾期且不提供退款。每次掃描沒有時間限制；掃描將會執行直到完成。  限制一次僅能執行三 (3) 項執行中的工作。 |
| **依應用程式的 AppScan** | |
| 訂閱類型 | 說明 |
| ASoC\_PerApplication | 年度訂閱，其依應用程式適當情況而定，使用任何掃描技術（Static Analyzer、Dynamic Analyzer 或 Mobile Analyzer）提供無限制的應用程式掃描（「應用程式實例」）。  限制一次僅能執行一 (1) 項執行中的工作。 |
| **AppScan 無限計價選項** | |
| 訂閱類型 | 說明 |
| AsoC\_PerConcurrent | 年度訂閱，其使用任何掃描技術（Static Analyzer、Dynamic Analyzer 或 Mobile Analyzer）提供任何應用程式掃描。  限制每次並行掃描授權執行一 (1) 項執行中的工作。  （「1」的並行實例） |
| ASoC Premium | 年度訂閱，其使用任何掃描技術（Static Analyzer、Dynamic Analyzer 或 Mobile Analyzer）提供高達十 (10) 項任何應用程式的並行掃描。  限制每次「最高級」授權執行高達十 (10) 項執行中的工作。  （「10」的並行實例） |
| ASoC\_PerConcurrent 及 ASoC\_Premium 可結合起來，以達到客戶可能提出的並行要求。 | |
| **依應用程式的 AppScan IAST Analyzer** | |
| 訂閱類型 | 說明 |
| ASoC\_IAST\_PerApplication | 年度訂閱提供一 (1) 項應用程式（「應用程式實例」）的無限 IAST 掃描。  限制一次僅能執行一 (1) 項執行中的 IAST 工作。 |
| **AppScan IAST Analyzer 無限計價選項** | |
| 訂閱類型 | 說明 |
| ASoC\_IAST\_PerConcurrent | 年度訂閱，其提供任何應用程式的 IAST 掃描。  限制每次並行掃描授權執行一 (1) 項執行中的 IAST 工作。  （「1」的並行實例） |
|  |  |
| **依應用程式的 AppScan Open Source Analyzer** | |
| 訂閱類型 | 說明 |
| ASoC\_OSA\_PerApplication | 年度訂閱，其提供一 (1) 項應用程式（「應用程式實例」）的無限開放原始碼掃描。  限制一次僅能執行一 (1) 項執行中的工作。 |
| **AppScan Open Source Analyzer 無限計價選項** | |
| 訂閱類型 | 說明 |
| ASoC\_OSA\_PerConcurrent | 年度訂閱，其提供任何應用程式的開放原始碼掃描。  限制每次並行掃描授權執行一 (1) 項執行中的工作。  （「1」的並行實例） |
| ASoC\_OSA\_Premium | 年度訂閱，其提供高達十 (10) 項任何應用程式的並行開放原始碼掃描。  限制每次「最高級」授權執行高達十 (10) 項執行中的工作。  （「10」的並行實例） |
|  | |

**3. 收費與計費**

HCL AppScan on Cloud 的應付金額會在訂單中指定。

**3.1 部分月份費用**

訂單中指定的部分月份費用可依照比例評估。

**3.2 計費頻率**

依所選的計費頻率為基礎，HCL 在計費頻率條款開始時將會開立發票告知客戶費用截止日，除了超額和費用使用類型將於欠款中開立發票。

**3.3 衍生權益位置**

依適用情況，稅金以確認客戶接收雲端服務權益的位置為基礎。除非客戶向 HCL 提供其他資訊，否則 HCL 將根據在訂購雲端服務做為主要權益位置時所列的營業地址來收取稅金。客戶有責任向 HCL 提供此類資訊的最新資訊與任何變更。

**3.4 驗證**

客戶將 i) 針對 HCL 與其獨立審核員而言合理且必要的情況下，維護並根據要求提供記錄和系統工具輸出，以驗證客戶對協議的合規性，以及 ii) 依照 HCL 當時費率盡速訂購與支付要求的授權量，並按照 HCL 在發票中指定的方式支付從此類驗證結果中確認的費用和賠償責任。這些合規驗證義務在雲端服務條款與往後兩年內皆保持其效力。

**4. 條款與續約選項**

雲端服務條款於 HCL 通知客戶可存取雲端服務的日期生效，記錄於授權書中。授權書將載明雲端服務是否自動續約，或在條款結束時終止。

針對自動續約，除非客戶在條款到期日前至少 30 天內以書面通知不續約，否則雲端服務將會依授權書中所述自動進行續約。

**技術支援**

在訂閱期間及 HCL 通知客戶雲端服務開放存取後，您可在 HCL 向客戶提供的 HCL 網站上取得技術支援資訊，也可以參照協議。

|  |  |  |  |
| --- | --- | --- | --- |
| **嚴重性** | **嚴重性定義** | **回應時間目標** | **回應時間涵蓋範圍** |
| 1 | 重要業務影響 / 服務中斷：業務的重要功能無法運作，或重要介面失敗。通常適用於正式作業環境，表示無法存取服務，對作業造成重大影響。此情況需要立即的解決方案。 | 1 小時內 | 全年無休 |
| 2 | 重要的業務影響：服務業務功能或此服務功能在使用上嚴重受限，或客戶面臨錯過業務截止時間的危險。 | 營業時間 2 小時內 | 週一至週五營業時間 |
| 3 | 次要業務影響：表示服務或功能可使用，作業上無嚴重影響。 | 營業時間 4 小時內 | 週一至週五營業時間 |
| 4 | 最小業務影響：查詢或非技術要求。 | 一個工作天 | 週一至週五營業時間 |

**5.1 存取客戶資料**

因診斷服務問題及協助服務掃描客戶應用程式等目的，HCL 將可存取客戶資料。HCL 僅為修正問題報告或提供 HCL 產品或服務的支援等目的而存取資料。

**6. 服務水準協議**

HCL 提供雲端服務的下列可用性服務水準協議（「SLA」）。SLA 並非保證書，是客戶唯一的專屬補救措施。SLA 僅向客戶開放，且僅可用於正式作業環境。

**6.1 可用性積分**

客戶必須在初次發現對業務產生重大影響並且無法使用雲端服務的 24 小時內，向 HCL 技術支援服務台上記錄「嚴重性 1」支援問題單。客戶必須合理協助 HCL 進行任何問題診斷與解決。

未滿足 SLA 要求的支援問題單務必於合約月份結束的 3 個工作天內提交。有效 SLA 要求的賠償將基於無法使用雲端服務正式作業系統處理的持續時間 （「停機時間」），而計入雲端服務未來發票的積分內。停機時間的量測方式是從客戶回報事件開始到雲端服務恢復為止，不包含與排程或公告維護中斷的相關時間；原因超出 HCL 的控制範圍；客戶或第三方內容或技術、設計或說明發生的問題；未支援的系統組態與平台或其他客戶錯誤；或客戶造成的安全意外或客戶安全測試。HCL 將會根據每個合約月份內雲端服務的累積可用性，套用最適用的補償，如下表所示。任何合約月份的總補償不得超過雲端服務年度費用的十二分之一 (1/12) 的百分之 10。

**6.2 服務層次**

合約月份內雲端服務的可用性

|  |  |
| --- | --- |
| **合約月份內的可用性** | **賠償（索賠對象之合約月份的月訂閱費用 \* 百分比）** |
| 低於 99.9% | 2% |
| 低於 99% | 5 |
| 低於 95% | 10% |

\* 如果從 HCL 業務夥伴方取得雲端服務，每月訂閱費用將根據雲端服務當時的標價計算，生效時間為索賠對象的合約月份，折扣率為 50%。HCL 將向客戶直接提供部分退款。可用性以百分比表示，計算方式如下：合約月份內的分鐘總數扣除合約月份內的停機時間分鐘總數，除以合約月份內的分鐘總數。

**技術預覽程式碼**

技術預覽程式碼 (TPC) 可能附隨於此程式或其更新檔，或與其併同配送，但其並非此程式之一部分。除下列規定者外，TPC 與此程式均依據相同條款進行授權。HCL 會在「注意事項檔案」中識別 TPC 檔案（或隨附於更新檔的更新注意事項檔案）。HCL 也許不會將部分 TPC 檔案做為產品或附於產品中向不特定人公開發布。被授權人僅可基於評估目的在內部使用 TPC。無論在購買時或購買前所做其他聲明為何，被授權人有責任確認此程式對於被授權人的網站、WEB 應用程式或技術環境是否適當或安全。被授權人知悉並接受與使用此程式相關的所有風險。注意事項檔案或概念證明協議 (POC) 可能會對評估用途設下評估期間限制。在此情況下，評估期間結束後，被授權人必須停止使用並解除安裝 TPC。HCL 以「現狀」提供來源元件及範例素材，惟其並無支援之義務，亦未提供任何種類之明示或默示保證，包括所有權、未侵權或未妨礙之保證，以及適售性與特定目的適用性的默示保證及條件。

除了隨附於本程式內一起轉讓以外，被授權人不得將 TPC 轉讓給其他方。本「程式」可能包含一個停用裝置， 以防止評估期滿後之使用。被授權人不得竄改該停用裝置或 TPC。被授權人應採取預防措施，以避免因不再使用 TPC 而可能造成之任何資料滅失。

**8. HCL AppScan on Cloud 補充條款**

**8.1 安全掃描**

安全掃描可能無法識別應用程式中的所有安全風險，也並非是為了在需要保全機制作業的危險環境中使用而設計或規劃，包括無限制的飛機導航、空中交通控制系統、武器系統、生命維持系統、核設施，或任何其他無法識別安全風險可能導致死亡、人員受傷或財產毀損的應用程式。安全掃描不保證不中斷作業，或不出現錯誤。

HCL AppScan on Cloud 可用於協助客戶達到合規義務，合規義務可能以法律、法規、標準或慣例為標準。任何服務提供的指示、建議使用方式或指南不代表法律、會計或其他專業建議，請客戶自行取得法律或其他專業諮詢。客戶需自行負責確保客戶與客戶的活動、應用程式及系統符合所有可套用的法律、法規、標準與慣例。使用此服務不保證遵守任何法律、法規、標準或慣例。

HCL AppScan on Cloud 會針對客戶選擇掃描的網站與 Web 或行動應用程式，進行侵入與非侵入式的測試。特定法律禁止任何未經授權方企圖進入或存取電腦系統。客戶將授權 HCL 依此處所描述執行服務，並且了解服務經授權可存取客戶的電腦系統。如果需要執行服務，HCL 可能會酌情向第三方披露此授權。測試代表特定程度的風險，包含但不限於下列：

客戶的電腦系統在測試期間執行應用程式時可能會當掉或毀損，導致系統暫時無法使用或資料遺失；

* 客戶系統的效能及傳輸量，以及相關路由器與防火牆的效能與傳輸量，可能在測試期間暫時遭到降級；
* 可能會產生過多日誌訊息，而消耗過多的日誌檔案磁碟空間；
* 資料可能因為探測漏洞而導致變更或刪除；
* 入侵偵測系統可能會觸發警示；
* 測試中的 Web 應用程式的電子郵件函數可能會觸發電子郵件；
* HCL AppScan on Cloud 可能會截取監控網路的流量，以尋找事件。

任何由 HCL 提供，且與測試中網站或應用程式相關的服務等級協議權利或補救措施將在任何測試活動中免除。

如果客戶將受測應用程式經鑑別的登入認證輸入服務中，客戶應僅為測試帳戶（而非為正式作業使用者）輸入此類認證。使用正式作業使用者認證可能會導致個人資料經由服務傳輸。

HCL AppScan on Cloud 可能會經配置進行掃描正式作業 Web 應用程式。當客戶將掃描類型設定為「正式作業」，服務旨在以降低上述風險的方式執行掃描；然而在特定情況中 HCL AppScan on Cloud 可能會在受測的正式作業網站與基礎設施中出現降級或不穩定狀態。HCL 不保證或代表使用 HCL AppScan on Cloud 掃描正式作業網站的適用性。

客戶應負責決定服務對客戶網站、WEB 應用程式、行動應用程式或技術環境是否適當或安全。

HCL AppScan on Cloud 旨在識別手機、Web 應用程式與 Web 服務的各種潛在安全與合規問題。其不測試所有漏洞或合規風險，亦不作為安全攻擊的屏障。安全威脅、法規與標準會持續變更，該服務可能無法針對所有此類變更作出相應措施。客戶的 Web 應用程式、系統與員工及任何補救行為的安全與合規性皆為客戶自行承擔責任。客戶需自行酌情使用或不使用服務提供的任何資訊。

特定法律禁止任何未經授權方企圖進入或存取電腦系統。客戶有責任確保除了客戶擁有或有權利與授權進行掃描的網站及 / 或應用程式之外，不使用服務掃描任何網站及 / 或應用程式。

為了清楚起見，CSA 的資料保護章節中所述的客戶內容，也視為在應用程式滲透測試期間包括 HCL 可能存取的資料。

**8.2 資料使用與 Cookie**

請在此處檢閱 HCL 隱私權聲明資訊：<https://www.hcltech.com/privacy-statement>

客戶了解並同意 HCL 作為 HCL AppScan on Cloud 的一般作業與支援的一部份，可能透過追蹤與其他技術從客戶（客戶的員工與承包商）方面收集與使用 HCL AppScan on Cloud 相關的個人資訊。HCL 用這個方式收集與 HCL AppScan on Cloud 效用有關的使用統計資料與資訊，以改善使用者體驗及 / 或為客戶量身訂製互動方式。客戶確認其將會取得或已取得客戶同意，允許 HCL 在符合適用法律的情況下，處理因上述目的而在 HCL 範圍內、其他 HCL 公司與其子公司以及 HCL 和其子公司營運之處蒐集到的個人資訊。HCL 將因應客戶員工與承包商的要求，存取、更新、更正或刪除其經收集的個人資訊。

作為 HCL AppScan on Cloud 的一部份（包括產生活動的報告），HCL 將準備與維護自 HCL AppScan on Cloud 收集的去識別化資訊和聚集資訊（稱為「安全資料」）。安全資料將無法識別客戶或個人，此處為例外情況。客戶在此

進一步同意 HCL 僅可因下列目的使用及 / 或複製安全資料：

* 發行及 / 或散佈安全資料（例如與網路安全相關的編譯及 / 或分析）；
* 開發或加強產品或服務；
* 內部或與第三方執行研究；及
* 合法共享已確認的第三方嫌犯資訊。

**8.3 啟用軟體**

雲端服務可能會要求使用客戶下載到客戶系統的啟用中軟體，以促進雲端服務的使用情形。客戶可使用下列的啟用軟體，此類軟體僅可用於與雲端服務使用情形相關的連線。啟用軟體以下列用語向客戶提供：

|  |  |
| --- | --- |
| **啟用軟體** | **適用的授權條款（若有）** |
| HCL AppScan on Cloud | 為依照原樣使用而提供 |
| AppScan Go! | 為依照原樣使用而提供 |
| AppScan Presence | 為依照原樣使用而提供 |
| AppScan IAST 代理程式 | 為依照原樣使用而提供 |