Onsites AI

DEPLOYMENT GUIDE · EDITION 2.0

地端部署指南

資料留在你自己的伺服器上

一套映象，兩種網路：可連外網，也可以完全離線。模型與儲存由你提供，我們不收這兩項費用；安裝、更新與支援由我們來做。



版本	釋出	支援系統	文件編號
第 2.0 版	2026 年 11 月	Linux · Windows · macOS	ONS-SH-TW-2.0

© 2026 Onsites AI · 本文件隨產品迭代更新，最新版本見 onsitesai.com/tw/download.html

目錄

CONTENTS

01 **什麼時候該地端** 三類組織、一張判斷表、什麼情況不必 03

02 **架構與資源要求** 一套映象、四段鏈路、離線與升級 04

03 **四步上線** 評估、安裝、接入、試點，各自的交付物 05

04 **授權、費用與責任** 價格結構、與雲端的差別、雙方邊界 06

一頁讀懂

$20 /席次/月
年付 $240
10 席次起

24 小時
安裝、配置與
遷移除錯用時

60 天
完整產品試點
跑完再買授權

0 元
AI 模型與儲存
我們都不收費

你的情況	建議形態	原因
客戶資料、通話記錄必須留在境內機房	地端部署	出境即違規的場景，只有資料不出網才成立。
生產車間、軍工或內網辦公，完全不連外網	地端部署（離線）	需要離線安裝與離線包升級，不能靠聯網啟用。
必須用自建模型與自有儲存	地端部署	模型、金鑰與磁碟都由自己提供，不買點數。
只是對隔離性有要求，仍希望我們運維	商業版 · 專屬雲	獨佔執行個體與駐留區域，但省掉機房與補丁。
常規團隊，先把話接起來	雲端 SaaS	15 秒開通，免費版即可驗證流程。

這張表覆蓋了絕大多數選型討論；更細的判斷見第 1 章。

文件用途

供 IT、安全與採購評估地端部署的可行性、資源與費用，可直接作為立項附件。

價格口徑

美元（USD），年付。最終報價以合約與訂單為準；調整會同步官網與本文件。

不包含

本指南不含客戶側網路與硬體的採購實施，也不替代等保、行業合規的第三方測評。

版本與回饋

第 2.0 版，2026 年 11 月。評估問題請傳送至 support@onsitesai.com。

01

WHEN TO SELF-HOST

三類組織，公有云解決不了的問題

地端不是「更貴的 SaaS」，而是給那些資料不能出網、或必須自己掌握 AI 與儲存的組織準備的。判斷標準很簡單：不是預算問題，而是資料能不能離開你的網路。

1.1 三類典型場景

場景一

資料不能出網

政府、銀行、醫療與政策嚴格的子公司：客戶資料、通話記錄與銷售單據必須留在境內、留在自己的機房，出境即為違規。

場景二

網路物理隔離

生產車間、軍工與內網辦公環境完全不連外網。軟體要能離線執行，也要能用離線包升級，而不是「先連網啟用一下」。

場景三

自建 AI 與儲存

模型、金鑰與檔案儲存都由自己提供：不買點數、不做用量計量，預設情況下客戶資料不離開你的網路。

1.2 一條主線：資料在哪

問題 01

資料能否離開你的網路?

不能 → 地端。能，但需要明確區域與隔離 → 專屬雲。都可以 → 雲端 SaaS。

問題 02

是否必須離線執行?

是 → 地端 + 離線包升級。否 → 三種形態都可以，按運維成本選。

問題 03

模型與金鑰誰提供?

自己提供 → 地端，我們不收 AI 與儲存費用。由平台統一呼叫 → 雲端或專屬雲。

問題 04

誰來做運維?

我們託管 → 雲端 / 專屬雲。你的機房團隊 + 我們的支援 → 地端。

圖 1-1　四個問題走完，形態基本就定了。任何一題答「必須自己掌握」，答案就收斂到地端。

1.3 什麼情況不必地端

- **只是擔心「資料安全」但沒有硬性約束。**雲端同樣有 TLS 1.3、靜態加密、席次許可權、工作區隔離與審計記錄，先看第 12 章（產品手冊）再做判斷。
- **團隊沒有機房與運維力量。**地端需要有人管伺服器、補丁與備份；沒有的話，專屬雲是更省事的折中——執行個體獨享、區域可選，仍由我們運維。
- **想先驗證流程。**雲端免費版就能跑通「一個佇列接所有通路」，驗證完再談部署形態，避免一次性投入。

> **一條經驗**　真正需要地端的組織，通常在第一次溝通時就會提到「出境」「等保」「內網」這三個詞。如果一個都沒提到，先從雲端或專屬雲開始，成本與風險都更低。

02

ARCHITECTURE

一套映象，四段鏈路

整套系统只有一個映象：沒有需要單獨維護的中介軟體，也沒有廠商繫結。雲主機與內網伺服器裝的是同一個映象，因此升級、備份與排障的方式完全一致。

2.1 部署拓撲



圖 2-1　四段鏈路。中間兩層完全在你的網路內；最後一層標註為可選——完全隔離的環境裡，模型端點可以在內網，通路出口可以只保留郵件。

2.2 資源清單

專案	要求
支援系統	Linux · Windows · macOS
最低配置	1 臺虛擬機器 · 4 核 · 8 GB 記憶體 · 3 Mbps 頻寬
網路	可連外網，也可完全離線；離線環境使用離線包升級
AI 模型	你的 API 金鑰、內部模型或物理隔離端點
儲存	你自己的磁碟，容量由你管理；聊天與郵件文字佔用極小，附件是主要消耗
備份	備份指令碼隨授權提供，按你的保留策略執行

2.3 離線與升級

- **離線安裝。**安裝包與依賴一起帶走，不需要在部署時聯網下載任何元件。
- **離線升級。**新版本以離線包交付，匯入後按引導完成升級；不要求「先連網啟用一下」。
- **排障方式一致。**雲端與內網用同一套日誌與健康檢查，出問題時我們看的是同一份資訊。
- **不發放自助安裝包。**部署由我們完成——一次裝錯拖累的是生產環境。

資源怎麼估　席次在 50 人以內、附件不堆到 TB 級時，4 核 8 GB 的單機足夠；席次數、併發會話與附件體量是三個主要變數。拿不準就把預期規模告訴我們，評估階段會給一份可直接採購的清單。

03

ROLLOUT

四步上線，每一步都有交付物

地端的風險不在軟體，而在「裝完之後沒人知道算不算裝好了」。所以四步裡每一步都約定交付物：評估給清單，安裝給可用環境，接入給聯調記錄，試點給一份可以拿去立項的結論。

3.1 四個步驟

STEP 01

環境評估

確認架構、資料駐留與隔離要求，給出可直接採購的資源清單。

STEP 02

安裝部署

支付一次性 $299 後由我們完成安裝、配置與資料遷移除錯，約 24 小時。

STEP 03

接入 AI 與儲存

填入自有模型金鑰或內網端點，指定磁碟位置；這兩項我們不收費。

STEP 04

試點與採購

完整產品跑 60 天，跑完再按席次購買授權，不必一開始承擔全年費用。

圖 3-1　四步上線。第三步與第四步的順序可以顛倒：也可以先試用、再接入模型。

3.2 交付物與時間

階段	用時	你提供	我們交付
環境評估	1–3 個工作天	網路與隔離要求、預期規模	資源清單、架構確認書、實施排期
安裝部署	約 24 小時	伺服器、網域與證書	可登入的環境、健康檢查報告
接入 AI 與儲存	半天	模型端點、金鑰、磁碟路徑	聯調記錄、呼叫連通性測試
試點	60 天	參與人員與真實業務	使用報告、容量建議、授權報價

3.3 試點期建議關注的三件事

- **先接一個通路。**網站聊天或主信箱，跑通「客戶進來 → 有人接 → 記錄留下」，再開第二個通路。
- **把單據跑一單。**報價 → 訂單 → 合約 → 發票走一遍真實業務，確認編號、稅率與審批能被複核。
- **給 AI 設上限。**先把 Copilot 開啟，Harness 與 Desk 按需；軟性上限跑兩週，再決定是否改硬性上限。

> **試點不等於壓測**　60 天試點用來驗證流程與接受度，不是效能壓測。如果預期峰值併發很高（例如大促期間的線上客服），請在評估階段就說明，我們會按峰值給資源建議。

04 LICENSING

授權、費用與責任邊界

席次價格裡已經包含軟體授權、軟體更新與技術支援。AI 模型與儲存由你自己提供，所以這條路線沒有 AI 費，也沒有儲存費——這三件事分開看，賬就很清楚。

4.1 價格結構

$20 /席次/月	$2,400 起	$299 一次	$0 AI/儲存
年付 $240 / 席次 最少 10 個席次	10 席次年費 起步價	安裝部署費 不抵扣授權費	模型與磁碟 由你提供

席次可隨時增加，按剩餘時間折算到續費日。安裝部署費在試用開始前支付，由我們完成安裝與除錯，單獨收取、不抵扣授權費。收款透過 2Checkout（Verifone）完成，可開據發票。

4.2 與雲端的三處差別

對比項	雲端（SaaS）	地端部署
開通時間	15 秒，無需安裝	約 24 小時，由我們安裝除錯
資料位置	Onsites 雲端；專屬雲可選區域	你的機房或你的私有云
離線執行	—	✓ 完全離線，用離線包升級
計費	$15 / 席次 / 月（年付 $180）	$20 / 席次 / 月（年付 $240），10 席次起
AI 與儲存	點數按需購買，儲存 $1/GB/月	由你提供，我們不收費
維護與升級	由我們託管運營	安裝、更新與技術支援由我們提供

同一套軟體、同一套功能。差異只有三處：資料放在哪、由誰維護、怎麼付費。

4.3 雙方的責任劃分

事項	客戶負責	我們負責
主機與網路	伺服器、儲存、網路與作業系統	軟體安裝、配置與升級支援
模型與金鑰	提供端點與金鑰，我們不持有	接入聯調與連通性排查
備份	按指令碼執行並保管備份介質	提供備份指令碼與恢復步驟
安全事件	主機與網路層的監控與處置	軟體層漏洞修復與通報

下一步 把環境說清楚（Docker / 虛擬機器、物理隔離、私有云 VPC），我們會在一個個工作天內給出可直接執行的部署答覆；試點從支付 $299 安裝部署費開始，跑完 60 天再決定是否購買授權。
評估申請：onsitesai.com/tw/self-host.html · 郵件：support@onsitesai.com