Onsites AI

SECURITY WHITEPAPER · EDITION 2.0

安全与数据驻留白皮书

数据在谁手里，写清楚

加密、访问控制、审计、备份与删除时间线、AI 数据边界与漏洞披露，逐项写明做法与责任方。不写「企业级安全」这类无法验证的形容词。



版本	发布	适用范围	文档编号
第 2.0 版	2026 年 11 月	云端 · 专属云 · 私有化	ONS-SC-ZH-2.0

© 2026 Onsites AI · 本文档随产品迭代更新，最新版本见 onsitesai.com/cn/download.html

目录

CONTENTS

01 **处理角色与数据边界** 谁控制、谁处理、AI 能碰到什么 …… 03

02 **加密、访问控制与审计** 九个控制点的具体做法 …… 04

03 **驻留、备份与生命周期** 数据放在哪、留多久、怎么删 …… 05

04 **安全问卷与披露流程** 常见问答、漏洞披露、联系方式 …… 06

摘要

Onsites AI 把客户数据当作客户托付的资产。云端与私有化两条路线都具备加密、访问控制与审计记录；选择私有化时，全部数据可以留在你自己的网络内。本文档逐项说明九个控制点的做法，并写明哪些由我们负责、哪些由客户负责——安全评估最怕的不是「有漏洞」，而是「说不清边界」。

9 项	TLS 1.3	1 个工作日	3 种形态
内置控制点 可逐条对应问卷	全站传输加密 静态存储同样加密	安全报告 确认时限	云端、专属云、 私有化各自边界

九个控制点一览

01 传输
TLS 1.3

02 静态
存储介质加密

03 密钥
与数据分开存放

04 权限
按席位授权，可收窄为只读

05 隔离
工作区之间互不可见

06 分享
外链可设有效期与次数

07 审计
操作人、时间与细节

08 备份
付费工作区自动备份，可导出

09 AI 边界
只读本工作区，不回训

文档用途

供安全评估、供应商问卷与合规审查使用，可作为答复附件直接提交。

适用范围

云端 SaaS、商业版 · 专属云与私有化部署三种形态；差异处已单独标注。

声明

本文档描述产品内置能力，不等同于第三方认证。等保、行业合规测评需另行委托。

版本与反馈

第 2.0 版，2026 年 11 月。勘误与安全报告请发送至 support@onsitesai.com。

01

ROLES & BOUNDARY

谁控制、谁处理、AI 能碰到什么

安全评估的第一个问题是角色：数据是谁的，谁在处理，处理过程中会不会交给第三方。Onsites AI 的角色划分很直接——客户是控制者，我们是处理者，子处理者只有基础设施与模型两类，且随部署形态变化。

1.1 三种角色

控制者

客户（你）

决定收集什么、保存多久、给谁看。工作区内的席位、角色与权限由你配置；导出与删除也由你发起。

处理者

Onsites AI

按你的配置处理数据：存储、检索、生成草稿与单据。不将数据用于自身目的，不跨工作区复用。

子处理者

基础设施与模型

云端形态下为云基础设施与我们调用的模型服务；私有化形态下这两类由客户自己提供，我们不持有。

1.2 一次 AI 调用的四个边界点

边界内

工作区数据

会话、客户、单据、文件。只有本工作区的成员按权限可见。

检索时

权限过滤

按发起人的席位权限裁剪可读范围；无权访问的记录不进入上下文。

推理时

模型调用

仅传输本次所需的最小上下文；私有化可指向内网端点，数据不出网。

返回后

答案与出处

结果标注引用的记录；不写入训练集，不跨工作区复用。

图 1-1　四个边界点。任何一环缺省，都不应把数据送进模型——这也是我们只读本工作区、且每条答案都要求标注来源的原因。

1.3 四条 AI 使用边界

- **只读本工作区。**Copilot、Harness、Agent Studio 与 Desk 在三种部署形态下都只读取当前工作区的数据，不跨工作区检索。
- **回答带出处。**每个答案标注它引用了哪条会话、哪个客户字段或哪份文件，便于复核；引用不到的，不写进答案。
- **不用于训练。**客户数据不会用于训练共享或公开模型。私有化部署下模型与密钥完全由客户提供，默认不出内网。
- **可整体关闭。**AI 能力可按工作区或成员关闭，关闭后其余功能完全正常，不进入降级状态。

1.4 三种形态下的角色差别

环节	云端 / 专属云	私有化部署
基础设施	我们运营；专属云为独享实例	客户自有机器与网络
模型与密钥	平台统一调用，密钥由我们管理	客户提供端点与密钥，我们不持有
数据位置	Onsites 基础设施；专属云可选区域	客户机房或私有云，可完全离线

同一套软件、同一套功能；角色划分的差别只来自「谁提供基础设施与模型」。

关于「我们看不看得到」　云端形态下，运维人员为排障可能接触到脱敏后的日志与错误信息；会话正文与附件不作为日常运维对象。若这一点不可接受，私有化部署是更彻底的选择——数据完全不出你的网络。

02

CONTROLS

九个控制点，逐项落到做法

安全问卷通常按控制点逐条问。下面按「加密 → 访问 → 记录 → 分享 → AI」的顺序给出做法与责任方，可以直接对照填写；三种形态的差异单独标注。

2.1 加密与密钥

环节	做法	谁负责
传输	全站 TLS 1.3；私有化由你的网关终止 TLS，证书由你管理	云端我们配置；私有化客户配置
静态存储	在我们基础设施上静态存储时加密；私有化时磁盘加密由你的操作系统与存储层完成	云端我们；私有化客户
密钥管理	密钥与数据分开存放，仅平台团队可访问	云端我们；私有化客户持有
备份介质	备份文件同样加密；备份目标位置由部署形态决定	见第 3 章

2.2 访问控制

- **按席位授权。**谁能看到什么由席位与角色决定；角色可收窄为只读，用于财务与管理层查看。
- **工作区隔离。**各工作区之间相互隔离，数据不跨工作区流动，AI 检索同样受限。
- **收回即时生效。**移除席位即同时收回访问权，不需要额外操作。
- **文件分享控制。**私有文件与文件夹，按受众分享给客户、合作伙伴或同事；外链可设有效期与打开次数上限，并可随时吊销。

2.3 审计与可追溯

文档与对话的状态变更都会记录操作人、时间与细节：谁把报价发给了客户、谁改了金额、谁确认了合同。日志随其他数据一同导出，因此几个月之后仍可作为审批依据，而不是只在系统里保留一段时间的「活动流」。Desk 执行的动作同样写入日志——读了什么、写了什么、花了多少点。

记录项	内容	用途
状态变更	单据与对话的状态流转	复核审批链，回答「这一版是谁发的」
权限变更	席位与角色的授予与收回	离职交接与审计取证
AI 执行	读取范围、写入结果、点数消耗	确认智能体没有越界

2.4 控制点落在链路的哪一段

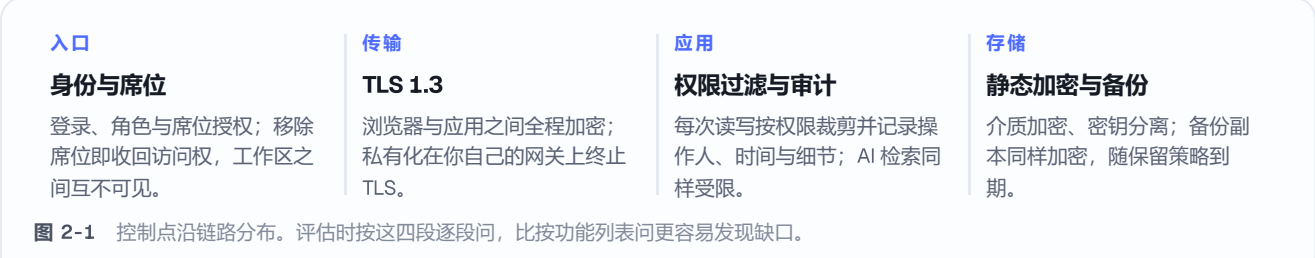


图 2-1 控制点沿链路分布。评估时按这四段逐段问，比按功能列表问更容易发现缺口。

怎么验证 评估阶段可以要求我们按上面三条各给一条真实样本（脱敏后）：一条状态变更、一条权限变更、一条 AI 执行记录。能给出样本，比在问卷上勾「是」更有说服力。

03

RESIDENCY

数据放在哪、留多久、怎么删

驻留问题通常有三个子问题：数据存在哪个区域、备份保留多久、终止合作后怎么删。前两个可以按部署形态选，第三个取决于你有没有导出——这也是我们反复强调「定期导出」的原因。

3.1 一条数据的生命周期



图 3-1　生命周期四段。真正需要提前约定的是最后一段：谁发起删除、备份副本保留多久、如何确认已删。

3.2 三种形态的驻留与备份

形态	数据位置	备份	删除
云端 SaaS	Onsites 基础设施	付费工作区自动备份	按请求执行，备份按保留策略到期
商业版 · 专属云	可选实例与备份区域，开通时固定	自动备份，区域随实例	同上，区域不变
私有化部署	你的机房或私有云	按随授权提供的脚本执行	由你执行；我们提供步骤与确认清单

区域在开通时固定，之后不会变更；如需迁移区域，按新实例迁移处理。

3.3 导出、降级与保留

- **导出是权利，不是功能开关。**对话、联系人与文档都能以标准格式导出，不锁定格式、不收取导出费。
- **降级不删数据。**停止存储包或降低套餐后，已存数据保留，按需再续；不会因为降级而丢失历史。
- **免费版没有服务端副本。**免费工作区不保留服务端备份，定期导出即是你唯一的副本——这一点最容易被忽略。
- **删除要能确认。**我们提供删除执行记录与备份到期时间，避免出现「说删了但备份还在」的争议。

3.4 保留策略怎么定

数据类别	建议保留	原因
会话与客户记录	与业务同周期	售后与复购判断都依赖历史对话，过早清理会丢上下文。
报价、合同与发票	按财税要求	通常长于会话；编号与金额需可复核，版本要留旧档。
审计日志	长于单据本身	审批与争议处理需要「谁在什么时候改了什么」。
备份副本	短于主数据	备份只为恢复，不必长期保留；到期即失效，避免删除争议。

以上是通用建议；实际保留期以你所在行业的监管要求为准。

建议写进合同的三个时间　① 数据导出可用的天数（终止后多久仍可取回）；② 备份副本的保留期；③ 删除完成后的书面确认时限。把这三个数字写清楚，比在问卷里勾「支持数据删除」有用得多。

04

QUESTIONNAIRE

安全问卷速查与漏洞披露

下面是供应商问卷里出现频率最高的几条，答案可以直接引用；更细的问题欢迎来信，我们会按你的问卷格式逐条填写，而不是回一份通用宣传材料。

4.1 常见问题

问题	答复
数据是否用于训练模型?	不。AI 只读本工作区数据，不用于训练共享或公开模型；私有化下模型由客户提供，数据默认不出内网。
是否支持指定数据存储区域?	商业版 · 专属云可指定实例与备份区域，开通时固定；云端为标准区域；私有化由客户决定。
员工能否看到客户会话内容?	云端运维出于排障可能接触脱敏日志；会话正文与附件不作为日常运维对象。需要更彻底的隔离请选私有化。
是否有审计日志? 能否导出?	有。状态变更、权限变更与 AI 执行均记录操作人、时间与细节，可随数据一同导出。
文件外链能否限制与吊销?	可以。按受众分享，设置有效期与打开次数上限，随时吊销。
终止合作后数据怎么处理?	以标准格式导出；删除按流程执行，我们会提供执行记录与备份到期时间。
AI 用量能否设上限?	可以。默认软性上限（接近额度时提醒、不中断），可改为硬性上限，达到即停止调用；点数用完时扣费自动暂停。
私有化环境能否离线升级?	可以。新版本以离线包交付，导入后按引导升级，不要求部署机联网激活。

4.2 漏洞披露

STEP 01

报告

发送至 support@onsitesai.com，直达开发该产品的团队。

STEP 02

确认

一个工作日内确认收到，并给出初判与联系人。

STEP 03

修复

按影响分级排期修复；期间保持进度同步，不等到发布才通知。

STEP 04

复盘

修复发布后同步结论；如涉及客户侧动作，会给出明确的操作清单。

图 4-1　披露流程。我们不设漏洞赏金，但会对报告者致谢（除非要求匿名）。

4.3 需要更多材料

如果你的评估需要特定格式的问卷回填、渗透测试报告或私有化环境的架构确认书，请直接说明格式与截止时间。私有化部署的客户还可以要求提供部署架构确认书，用于内部安全评审归档。

4.4 相关文档

文档	编号	用途
产品手册	ONS-PM-ZH-2.0	产品构成、能力范围、部署形态与价格结构（21 页）。
私有化部署指南	ONS-SH-ZH-2.0	私有化的适用场景、架构、资源与费用（6 页）。
安全与数据驻留白皮书	**ONS-SC-ZH-2.0**	本文档，供安全问卷与合规审查使用（6 页）。

三份文档均可从 onsitesai.com/cn/download.html 免费下载，不留表单。

联系方式　安全与合规：support@onsitesai.com（安全报告走同一地址，一个工作日内确认）
产品与文档：onsitesai.com/cn/download.html　·　私有化评估：onsitesai.com/cn/self-host.html