Onsites AI

SECURITY WHITEPAPER · EDITION 2.0

Sách trắng Bảo mật và Lưu trú Dữ liệu

Dữ liệu nằm trong tay ai, ghi rõ ràng

Mã hóa, kiểm soát truy cập, kiểm toán, sao lưu và mốc thời gian xóa, ranh giới dữ liệu của AI và báo lỗ hổng bảo mật — từng hạng mục đều nêu rõ cách làm và bên chịu trách nhiệm. Không dùng những tính từ không thể kiểm chứng như “bảo mật cấp doanh nghiệp”.



Phiên bản
Bản 2.0

Phát hành
Tháng 11 năm 2026

Phạm vi áp dụng
Cloud · Cloud riêng · Self-hosted

Mã tài liệu
ONS-SC-VI-2.0

© 2026 Onsites AI · Tài liệu này được cập nhật theo từng phiên bản sản phẩm; bản mới nhất tại onsitesai.com/vn/download.html

Mục lục

CONTENTS

01 **Vai trò xử lý và ranh giới dữ liệu** Ai kiểm soát, ai xử lý, AI được chạm tới đâu 03

02 **Mã hóa, kiểm soát truy cập và kiểm toán** Cách làm cụ thể của chín điểm kiểm soát 04

03 **Lưu trú, sao lưu và vòng đời dữ liệu** Dữ liệu ở đâu, lưu bao lâu, xóa thế nào 05

04 **Bảng hỏi bảo mật và quy trình công bố** Câu hỏi thường gặp, báo lỗ hổng bảo mật, thông tin liên hệ 06

Tóm tắt

Onsites AI coi dữ liệu khách hàng là tài sản mà khách hàng giao phó. Cả hai hướng cloud và self-hosted đều có mã hóa, kiểm soát truy cập và nhật ký kiểm toán; khi chọn self-hosted, toàn bộ dữ liệu có thể nằm trong mạng của chính bạn. Tài liệu này trình bày từng hạng mục trong chín điểm kiểm soát, kèm rõ bên nào chịu trách nhiệm — điều đáng ngại nhất khi đánh giá bảo mật không phải là "có lỗ hổng", mà là "không nói rõ được ranh giới".

9 hạng mục
Điểm kiểm soát có sẵn đối chiếu được từng dòng bảng hỏi

TLS 1.3
Mã hóa khi truyền toàn hệ thống
dữ liệu lưu trữ cũng được mã hóa

1 ngày làm việc
Thời hạn xác nhận báo cáo bảo mật

3 hình thức
Cloud, cloud riêng, self-hosted với ranh giới riêng

Tổng quan chín điểm kiểm soát

01 Truyền
TLS 1.3

02 Lưu trữ
Mã hóa vật mang lưu trữ

03 Khóa
Lưu tách biệt với dữ liệu

04 Quyền
Cấp quyền theo ghế, thu hẹp được về chỉ đọc

05 Cô lập
Các không gian làm việc không thấy nhau

06 Chia sẻ
Liên kết ngoài đặt được thời hạn và số lần mở

07 Kiểm toán
Người thực hiện, thời gian và chi tiết

08 Sao lưu
Không gian làm việc trả phí sao lưu tự động, xuất được

09 Ranh giới AI
Chỉ đọc không gian làm việc này, không huấn luyện lại

MỤC ĐÍCH TÀI LIỆU

Dùng cho đánh giá bảo mật, bảng hỏi nhà cung cấp và rà soát tuân thủ; gửi trực tiếp làm phụ lục cho câu trả lời được.

PHẠM VI ÁP DỤNG

Ba hình thức: cloud SaaS, bản thương mại · cloud riêng và triển khai self-hosted; chỗ khác biệt ghi chú riêng.

LƯU Ý

Mô tả năng lực có sẵn của sản phẩm, không đồng nghĩa chứng nhận của bên thứ ba. Đánh giá tuân thủ theo ngành và cấp độ bảo mật cần đặt riêng.

PHIÊN BẢN VÀ PHẢN HỒI

Bản 2.0, tháng 11 năm 2026. Đính chính và báo cáo bảo mật xin gửi tới support@onsitesai.com.

01

ROLES & BOUNDARY

Ai kiểm soát, ai xử lý, AI được chạm tới đâu

Đánh giá bảo mật hỏi trước hết về vai trò: dữ liệu của ai, ai xử lý, có chuyển cho bên thứ ba không. Onsites AI phân vai trực tiếp — khách hàng kiểm soát dữ liệu, chúng tôi xử lý dữ liệu; bên xử lý phụ chỉ gồm hạ tầng và mô hình, tùy hình thức triển khai.

1.1 Ba vai trò

Bên kiểm soát

Khách hàng (bạn)

Quyết định thu thập gì, lưu bao lâu, cho ai xem; bạn cấu hình ghế, vai trò, quyền trong không gian làm việc. Xuất và xóa cũng do bạn khởi tạo.

Bên xử lý

Onsites AI

Xử lý dữ liệu theo cấu hình của bạn: lưu trữ, tra cứu, tạo bản nháp và chứng từ; không dùng cho mục đích riêng, không tái sử dụng giữa các không gian làm việc.

Bên xử lý phụ

Hạ tầng và mô hình

Cloud: hạ tầng và dịch vụ mô hình chúng tôi gọi tới. Self-hosted: hai loại này do khách hàng cung cấp, chúng tôi không nắm giữ.

1.2 Bốn điểm ranh giới trong một lần gọi AI

Trong ranh giới

Dữ liệu không gian làm việc

Hội thoại, khách hàng, chứng từ, tệp. Chỉ thành viên của không gian làm việc này thấy theo quyền.

Khi tra cứu

Lọc theo quyền

Cắt phạm vi đọc theo quyền của ghế người khởi tạo; bản ghi không có quyền không vào ngữ cảnh.

Khi suy luận

Gọi mô hình

Chỉ truyền ngữ cảnh tối thiểu cho lần này; self-hosted trỏ được tới endpoint nội bộ, dữ liệu không ra khỏi mạng.

Sau khi trả kết quả

Câu trả lời và nguồn

Kết quả ghi rõ bản ghi được trích; không vào tập huấn luyện, không tái sử dụng giữa các không gian làm việc.

Hình 1-1 Bốn điểm ranh giới. Thiếu một khâu, dữ liệu không nên vào mô hình — cũng là lý do chúng tôi chỉ đọc không gian làm việc hiện tại và buộc mọi câu trả lời ghi nguồn.

1.3 Bốn ranh giới sử dụng AI

- **Chỉ đọc không gian làm việc hiện tại.** Copilot, Harness, Agent Studio và Desk ở cả ba hình thức đều chỉ đọc dữ liệu của không gian làm việc hiện tại, không tra cứu xuyên không gian.
- **Câu trả lời có nguồn.** Mỗi câu ghi rõ đã trích hội thoại, trường khách hàng hay tệp nào để đối chiếu; không trích được thì không đưa vào.
- **Không dùng để huấn luyện.** Dữ liệu khách hàng không dùng cho mô hình chia sẻ hoặc công khai; với self-hosted, mô hình và khóa do khách hàng cung cấp, mặc định không ra khỏi mạng nội bộ.
- **Có thể tắt toàn bộ.** AI tắt được theo không gian làm việc hoặc theo thành viên; sau khi tắt, các chức năng khác vẫn bình thường.

1.4 Khác biệt về vai trò giữa ba hình thức

Khâu	Cloud / Cloud riêng	Triển khai self-hosted
Hạ tầng	Chúng tôi vận hành; cloud riêng dùng phiên bản riêng	Máy chủ và mạng của khách hàng
Mô hình và khóa	Nền tảng gọi tập trung, khóa do chúng tôi quản lý	Khách hàng cung cấp endpoint và khóa
Vị trí dữ liệu	Hạ tầng Onsites; cloud riêng chọn được khu vực	Phòng máy hoặc cloud riêng của khách hàng, có thể ngoại tuyến

Cùng một bộ phần mềm, cùng một bộ chức năng; khác biệt phân vai chỉ ở “ai cung cấp hạ tầng và mô hình”.

Về việc “chúng tôi có thấy dữ liệu hay không” Hình thức cloud: nhân sự vận hành khi xử lý sự cố có thể tiếp xúc nhật ký và thông tin lỗi đã ẩn danh; nội dung hội thoại, tệp đính kèm không thuộc đối tượng vận hành. Không chấp nhận được thì chọn self-hosted.

02

CONTROLS

Chín điểm kiểm soát, từng hạng mục cụ thể

Bảng hỏi bảo mật hỏi theo từng điểm kiểm soát; chương này trả lời cùng thứ tự: mã hóa, truy cập, ghi nhật ký, chia sẻ, AI. Mỗi dòng nêu cách làm và bên chịu trách nhiệm.

2.1 Mã hóa và khóa

Khâu	Cách làm	Bên chịu trách nhiệm
Khi truyền	TLS 1.3 toàn hệ thống; self-hosted: TLS và chứng chỉ do proxy của bạn	Cloud: chúng tôi; self-hosted: khách hàng
Dữ liệu lưu trữ	Mã hóa trên kho của chúng tôi; trên đĩa của bạn do hệ điều hành lo	Cloud: chúng tôi; self-hosted: khách hàng
Quản lý khóa	Khóa tách biệt khỏi dữ liệu; chỉ nhóm nền tảng truy cập	Cloud: chúng tôi giữ; self-hosted: khách hàng giữ
Vật mang sao lưu	Tệp sao lưu cũng mã hóa; đích đến tùy hình thức triển khai	Xem Chương 3

2.2 Kiểm soát truy cập

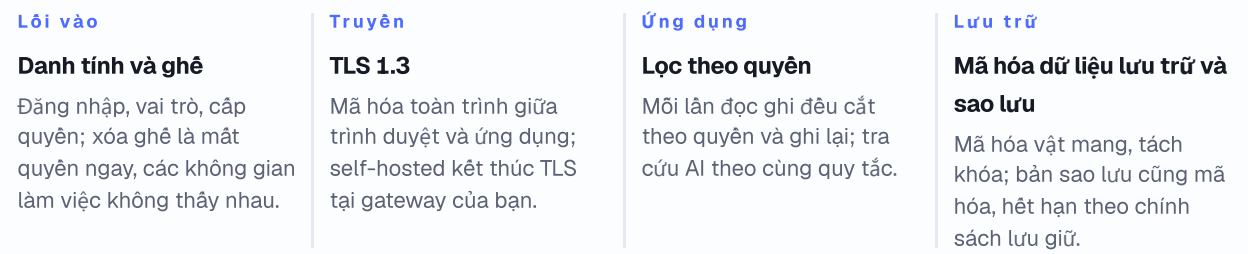
- **Cấp quyền theo ghế.** Người thấy gì theo ghế và vai trò; vai trò thu hẹp được về chỉ đọc cho tài chính, quản lý.
- **Cô lập không gian làm việc.** Các không gian làm việc không thấy nhau; dữ liệu không chuyển giữa chúng, AI cũng bị giới hạn như vậy.
- **Thu hồi tức thì.** Xóa ghế là mất quyền truy cập ngay, không cần thao tác thêm.
- **Chia sẻ có kiểm soát.** Tệp, thư mục riêng chia sẻ theo đối tượng; liên kết ngoài có hạn dùng, số lần mở và thu hồi bất cứ lúc nào.

2.3 Kiểm toán và khả năng truy vết

Mọi thay đổi trạng thái của tài liệu, hội thoại đều ghi người thực hiện, thời gian, chi tiết: ai gửi báo giá, ai sửa số tiền, ai xác nhận hợp đồng. Nhật ký xuất cùng dữ liệu nên vẫn làm được căn cứ phê duyệt sau vài tháng, không chỉ là dòng hoạt động tạm thời. Thao tác của Desk cũng vào nhật ký: đọc gì, ghi gì, tốn bao nhiêu điểm.

Hạng mục ghi	Nội dung	Mục đích
Thay đổi trạng thái	Chuyển trạng thái chứng từ, hội thoại	Đối chiếu chuỗi phê duyệt: “bản này do ai gửi”
Thay đổi quyền	Cấp, thu hồi ghế và vai trò	Bàn giao khi nghỉ việc, thu chứng cứ
AI thực thi	Phạm vi đọc, kết quả ghi, điểm đã dùng	Xác nhận AI không vượt ranh giới

2.4 Điểm kiểm soát nằm ở đoạn nào của chuỗi



Hình 2-1 Các điểm kiểm soát dọc chuỗi. Đi bốn đoạn này khi đánh giá tìm thiếu sót nhanh hơn đi danh sách chức năng.

Cách kiểm chứng Xin mỗi mục một mẫu đã ẩn danh: một thay đổi trạng thái, một thay đổi quyền, một bản ghi AI thực thi. Mẫu thật thuyết phục hơn đánh dấu “có” trên bảng hỏi.

03

RESIDENCY

Dữ liệu ở đâu, lưu bao lâu, xóa thế nào

Lưu trú dữ liệu gồm ba câu hỏi con: dữ liệu ở khu vực nào, bản sao lưu giữ bao lâu, xóa thế nào sau khi chấm dứt hợp tác. Hai câu đầu chọn theo hình thức triển khai; câu thứ ba phụ thuộc việc bạn có xuất dữ liệu — cũng là lý do chúng tôi nhấn mạnh "xuất định kỳ".

3.1 Vòng đời của một bản ghi dữ liệu

Tạo

Ghi vào không gian làm việc

Hội thoại, khách hàng, chứng từ, tệp nằm trong không gian làm việc, hiện theo quyền.

Sử dụng

Đọc ghi hằng ngày

Nhóm và AI cùng đọc ghi trên một bản ghi; mỗi thao tác ghi đều để lại dấu vết.

Sao lưu

Bản sao mã hóa

Không gian làm việc cloud trả phí sao lưu tự động; self-hosted chạy theo script, vật mang do bạn giữ.

Xuất / Chấm dứt

Mang đi hoặc xóa

Xuất theo định dạng chuẩn; xóa theo quy trình, bản sao lưu hết hạn theo chính sách.

Hình 3-1 Bốn đoạn vòng đời. Đoạn cần thỏa thuận trước là đoạn cuối: ai khởi tạo việc xóa, bản sao lưu giữ bao lâu, xác nhận đã xóa cách nào.

3.2 Lưu trú và sao lưu ở ba hình thức

Hình thức	Vị trí dữ liệu	Sao lưu	Xóa
Cloud SaaS	Hạ tầng Onsites	Trả phí: tự động	Theo yêu cầu, hết hạn theo chính sách
Bản thương mại · Cloud riêng	Chọn khu vực phiên bản, cố định khi kích hoạt	Tự động, khu vực theo phiên bản	Như trên, khu vực không đổi
Triển khai self-hosted	Phòng máy hoặc cloud riêng của bạn	Theo script kèm giấy phép	Bạn thực hiện; chúng tôi cho các bước và danh mục xác nhận

Khu vực cố định khi kích hoạt; cần chuyển khu vực thì xử lý như chuyển sang phiên bản mới.

3.3 Xuất, hạ gói và lưu giữ

- **Xuất dữ liệu là quyền, không phải công tắc.** Hội thoại, liên hệ và tài liệu đều xuất được theo định dạng chuẩn, không khóa định dạng, không thu phí.
- **Hạ gói không xóa dữ liệu.** Dừng gói lưu trữ hoặc hạ gói thì dữ liệu đã lưu vẫn còn, gia hạn khi cần; lịch sử không mất.
- **Bản miễn phí không có bản sao phía máy chủ.** Xuất định kỳ là bản sao duy nhất — điểm dễ bị bỏ qua nhất.
- **Xóa phải xác nhận được.** Chúng tôi cung cấp bản ghi thực hiện xóa và thời điểm bản sao lưu hết hạn, tránh tranh cãi "nói đã xóa mà vẫn còn".

3.4 Xác định chính sách lưu giữ thế nào

Loại dữ liệu	Lưu giữ đề xuất	Lý do
Hội thoại, hồ sơ khách hàng	Cùng chu kỳ kinh doanh	Hậu mãi và mua lại dựa vào hội thoại lịch sử; xóa sớm sẽ mất ngữ cảnh.
Báo giá, hợp đồng, hóa đơn	Theo yêu cầu tài chính, thuế	Thường dài hơn hội thoại; số hiệu, số tiền phải đối chiếu được.
Nhật ký kiểm toán	Dài hơn chứng từ	Phê duyệt và xử lý tranh chấp cần biết "ai sửa gì, khi nào".
Bản sao lưu	Ngắn hơn dữ liệu chính	Chỉ để khôi phục; hết hạn là mất hiệu lực, tránh tranh cãi khi xóa.

Trên đây là đề xuất chung; thời gian lưu giữ thực tế theo yêu cầu quản lý của ngành bạn.

Ba mốc thời gian nên ghi vào hợp đồng ① Số ngày còn xuất được dữ liệu (chấm dứt xong bao lâu vẫn lấy lại được); ② Thời hạn lưu giữ bản sao lưu; ③ Thời hạn xác nhận bằng văn bản sau khi xóa xong.

04

QUESTIONNAIRE

Tra nhanh bảng hỏi bảo mật

Dưới đây là những câu xuất hiện nhiều nhất trong bảng hỏi nhà cung cấp, trích dẫn trực tiếp được; câu chi tiết hơn xin gửi thư, chúng tôi điền từng dòng theo đúng mẫu của bạn.

4.1 Câu hỏi thường gặp

Câu hỏi	Trả lời
Dữ liệu có dùng để huấn luyện mô hình không?	Không. AI chỉ đọc dữ liệu của không gian làm việc hiện tại, không dùng cho mô hình chia sẻ hoặc công khai; với self-hosted, mô hình do khách hàng cung cấp, dữ liệu không ra khỏi mạng nội bộ.
Có chỉ định được khu vực lưu trữ không?	Bản thương mại · cloud riêng chỉ định được khu vực phiên bản và sao lưu, cố định khi kích hoạt; cloud dùng khu vực tiêu chuẩn; self-hosted do khách hàng quyết định.
Nhân viên có xem được hội thoại của khách hàng không?	Nhân sự vận hành cloud khi xử lý sự cố có thể tiếp xúc nhật ký đã ẩn danh; nội dung hội thoại và tệp đính kèm không thuộc đối tượng vận hành. Cần cô lập triệt để hơn, chọn self-hosted.
Có nhật ký kiểm toán không? Xuất được không?	Có. Thay đổi trạng thái, thay đổi quyền và AI thực thi đều ghi người thực hiện, thời gian, chi tiết và xuất được cùng dữ liệu.
Liên kết ngoài có giới hạn, thu hồi được không?	Được. Chia sẻ theo đối tượng, đặt thời hạn và số lần mở tối đa, thu hồi bất cứ lúc nào.
Chấm dứt hợp tác thì dữ liệu xử lý thế nào?	Xuất theo định dạng chuẩn; xóa theo quy trình, kèm bản ghi thực hiện và thời điểm bản sao lưu hết hạn.
Có đặt hạn mức sử dụng AI không?	Được. Mặc định hạn mức mềm (nhắc khi gần đạt, không ngắt), đổi được sang hạn mức cứng, đạt là dừng gọi; hết điểm thì tạm dừng trừ phí.
Self-hosted có nâng cấp ngoại tuyến không?	Được. Bản mới giao dạng gói ngoại tuyến, nhập vào rồi nâng cấp theo hướng dẫn, không cần máy triển khai có mạng.

4.2 Báo lỗ hổng bảo mật

STEP 01

Báo cáo

Gửi tới support@onsitesai.com, đến thẳng nhóm phát triển sản phẩm.

STEP 02

Xác nhận

Xác nhận trong một ngày làm việc, kèm đánh giá sơ bộ và người liên hệ.

STEP 03

Khắc phục

Lên lịch theo mức ảnh hưởng; vẫn cập nhật tiến độ, không đợi đến lúc phát hành.

STEP 04

Tổng kết

Sau khi phát hành, thông báo kết luận; nêu có việc phía khách hàng, đưa danh mục thao tác.

Hình 4-1 Quy trình công bố. Chúng tôi không có chương trình thưởng lỗ hổng, nhưng ghi nhận người báo cáo (trừ khi yêu cầu ẩn danh).

4.3 Cần thêm tài liệu

Nếu đợt đánh giá cần điền bảng hỏi theo mẫu riêng, báo cáo kiểm thử xâm nhập hoặc văn bản xác nhận kiến trúc cho môi trường self-hosted, hãy nêu rõ định dạng và thời hạn. Khách hàng self-hosted còn có thể yêu cầu văn bản xác nhận kiến trúc để lưu hồ sơ đánh giá nội bộ.

4.4 Tài liệu liên quan

Tài liệu	Mã số	Mục đích
Hướng dẫn sản phẩm	ONS-PM-VI-2.0	Cấu thành, phạm vi năng lực, hình thức triển khai, cơ cấu giá (21 trang).
Hướng dẫn triển khai self-hosted	ONS-SH-VI-2.0	Tình huống áp dụng, kiến trúc, tài nguyên, chi phí (6 trang).
Sách trắng Bảo mật và Lưu trú Dữ liệu	**ONS-SC-VI-2.0**	Tài liệu này, cho bảng hỏi bảo mật và rà soát tuân thủ (6 trang).

Cả ba tài liệu tải miễn phí tại onsitesai.com/vn/download.html, không cần để lại biểu mẫu.

Thông tin liên hệ Bảo mật và tuân thủ: support@onsitesai.com (báo cáo bảo mật dùng địa chỉ này, xác nhận trong một ngày làm việc)
Sản phẩm và tài liệu: onsitesai.com/vn/download.html · Self-hosted: onsitesai.com/vn/self-host.html