AI NATIVE LAB RESEARCH BRIEF

PREVIEW SAMPLE

Hermes Agent

AI NATIVE LAB

HERMES AGENT • AI OPERATING SYSTEM • 2026

AI NATIVE LAB PREVIEW

Hermes Agent

Tác giả: AI Native Lab

MỤC LỤC

Mục lục

CHƯƠNG 1

01

Hermes Agent

Từ chatbot biết trả lời đến AI OS biết vận hành

Preview bản mới — dùng để duyệt hướng nội dung, style và design trước khi viết toàn bộ

AI Native Lab

> **DÀNH CHO AI?**
> *CEO, founder, chủ doanh nghiệp SME và đội ngũ vận hành muốn hiểu Hermes Agent ở mức đủ sâu để ra quyết định: nên dùng để làm gì, triển khai thế nào, kiểm soát rủi ro ra sao, và vì sao nó khác chatbot thông thường.*

CHƯƠNG 2

02

Cover Direction

Concept: một cuốn e-book business-tech cao cấp, không "khoe AI", không viễn tưởng, không salesy. Hermes Agent được trình bày như một lớp vận hành mới cho doanh nghiệp: có trí nhớ, có kỹ năng, có lịch chạy tự động, có khả năng làm việc qua nhiều kênh, nhưng vẫn cần con người làm người duyệt cuối.

Visual language:

- Nền ivory ấm, chữ đen nâu, accent vàng đồng và đỏ rượu.
- Typography editorial: Playfair Display cho tiêu đề, Lora cho thân bài, Be Vietnam Pro cho nhãn, checklist, caption.
- Mỗi chương có ít nhất 2–3 element để phá nhịp: executive box, sơ đồ hệ thống, checklist, decision table, case card, warning box.

DESIGN PRINCIPLE

Không biến e-book thành brochure. Mỗi visual/ component phải giúp người đọc hiểu nhanh hơn, ra quyết định tốt hơn, hoặc nhớ được một ý quan trọng hơn.

CHƯƠNG 3

03

Mục lục đề xuất

1. **Vấn đề thật không phải là thiếu AI, mà là quá nhiều AI rời rạc**
   Vì sao doanh nghiệp dùng nhiều công cụ AI nhưng vẫn chưa vận hành nhanh hơn.

2. **Hermes Agent là gì?**
   Giải thích bằng ngôn ngữ CEO: agent có trí nhớ, có kỹ năng, có công cụ, có khả năng tự cải thiện.

3. **Từ chatbot đến AI Operating System**
   Khác biệt giữa "hỏi đáp" và "giao việc để hệ thống thực thi".

4. **Bốn năng lực lõi của Hermes Agent**
   Memory, Skills, Tools, Async Orchestration.

5. **CEO AI OS: biến Hermes thành lớp vận hành doanh nghiệp**
   Cách một công ty nhỏ dùng một agent framework để điều phối việc thật.

CHƯƠNG 4

04

Lời mở đầu

Nhiều doanh nghiệp bước vào AI bằng cách mua thêm công cụ.

Một công cụ để viết content. Một công cụ để tóm tắt họp. Một công cụ để làm ảnh. Một công cụ để phân tích dữ liệu. Một công cụ để chăm sóc khách hàng. Sau vài tháng, CEO phát hiện một nghịch lý: công cụ nhiều hơn, nhưng việc vẫn rời rạc; output nhiều hơn, nhưng quyết định chưa chắc nhanh hơn; automation nhiều hơn, nhưng người lãnh đạo vẫn phải ngồi ở giữa để nối từng mảnh lại với nhau.

Đây là điểm mà chatbot bắt đầu chạm trần.

Chatbot giỏi trả lời. Nhưng doanh nghiệp không chỉ cần câu trả lời. Doanh nghiệp cần một hệ thống có thể nhớ bối cảnh, dùng đúng công cụ, chạy việc theo lịch, gọi sub-agent khi cần, học lại quy trình sau mỗi lần làm, và ngày mai thực thi tốt hơn hôm nay.

Hermes Agent, dự án open-source của Nous Research, đáng chú ý vì nó không chỉ được thiết kế như một giao diện chat với model AI. Nó được thiết kế như một agent runtime: một lớp vận hành

nơi memory, skills, tools, cron jobs, delegation, execution backend và nhiều kênh giao tiếp cùng nằm trong một kiến trúc thống nhất.

Nói đơn giản hơn: nếu ChatGPT giống một chuyên viên rất giỏi nhưng hay quên khi mở cuộc trò chuyện mới, thì Hermes Agent giống một nhân sự vận hành có sổ tay, có lịch làm việc, có quyền dùng công cụ, có khả năng ghi lại cách làm, và có thể xuất hiện ngay trong nơi đội ngũ đang làm việc như Telegram, Slack, Discord hoặc email.

> **EXECUTIVE TAKEAWAY**
>
> *Câu hỏi chiến lược không phải là "Hermes có thông minh hơn model A hay model B không?". Câu hỏi đúng hơn là: "Doanh nghiệp có cần một lớp vận hành AI có trí nhớ, kỹ năng, công cụ và kỷ luật thực thi hay không?".*

E-book này không viết cho kỹ sư muốn đọc tài liệu API từ đầu đến cuối. Nó viết cho CEO, founder và chủ doanh nghiệp muốn hiểu đủ sâu để ra quyết định: Hermes Agent có đáng quan tâm không, nên áp dụng vào đâu trước, rủi ro nằm ở đâu, và làm sao triển khai mà không biến công ty thành một mớ thử nghiệm AI hỗn loạn.

CHƯƠNG 5

05

Chương mẫu: Hermes Agent là gì?

Nếu nhìn bề mặt, Hermes Agent có thể giống một chatbot nâng cao: bạn nhắn một yêu cầu, nó trả lời hoặc làm việc giúp bạn. Nhưng nếu chỉ nhìn như vậy, ta sẽ bỏ lỡ điểm quan trọng nhất.

Hermes không chỉ là "một con bot". Hermes là một hệ điều phối agent.

Nó kết hợp nhiều lớp năng lực mà các chatbot phổ thông thường tách rời hoặc không có sẵn: trí nhớ dài hạn, kỹ năng dạng tài liệu có thể tái sử dụng, công cụ để thao tác với thế giới bên ngoài, môi trường chạy lệnh, cơ chế giao việc nền, sub-agent độc lập, và khả năng hiện diện trên nhiều nền tảng nhắn tin.

Sơ đồ 1: Từ prompt đơn lẻ đến hệ điều phối AI

LỚP	CHATBOT THÔNG THƯỜNG	HERMES AGENT
Bối cảnh	Phụ thuộc vào nội dung trong cuộc chat hiện tại	Có memory và session recall để nhớ qua nhiều phiên
Cách làm việc	Trả lời từng lượt	Có thể chạy workflow nhiều bước
Quy trình	Người dùng phải nhắc lại	Có Skills để lưu cách làm thành playbook
Công cụ	Giới hạn trong giao diện	Có toolsets, terminal, browser, file, cron, message gateway
Kênh sử dụng	Thường nằm trong một app	Có thể sống trong Telegram, Discord, Slack, email và nhiều kênh khác
Cải thiện theo thời gian	Chủ yếu do người dùng prompt tốt hơn	Có thể tạo/sửa skills sau khi hoàn thành việc phức tạp

> **KEY IDEA**
>
> *Điểm khác biệt của Hermes không nằm ở một câu trả lời hay hơn. Điểm khác biệt nằm ở khả năng biến kinh nghiệm làm việc thành tài sản vận hành có thể dùng lại.*

Bốn thành phần dễ hiểu nhất

1. MEMORY — ĐỂ AI KHÔNG BẮT ĐẦU LẠI TỪ SỐ 0

Trong doanh nghiệp, phần mệt nhất khi dùng AI không phải lúc nào cũng là viết prompt. Phần mệt nhất là phải giải thích lại bối cảnh: công ty làm gì, khách hàng là ai, giọng thương hiệu ra sao, dự án đang ở đâu, ai là người duyệt cuối, dữ liệu nào được phép dùng, dữ liệu nào không.

Hermes giải quyết vấn đề này bằng nhiều tầng nhớ: memory ngắn cho phiên hiện tại, memory dài cho thông tin bền vững, và cơ chế tìm lại phiên cũ khi cần. Nhờ vậy, AI không chỉ trả lời dựa trên câu hỏi vừa nhận, mà có thể làm việc dựa trên lịch sử và quy ước đã được tích lũy.

> **COMPONENT MẪU: MEMORY CARD**
> **CẦN LƯU:** *preference ổn định, quy ước công ty, workflow lặp lại, cấu hình môi trường.*
> **KHÔNG NÊN LƯU:** *việc đã xong, số liệu dễ hết hạn, link tạm, quyết định chưa duyệt, chi tiết riêng tư không cần thiết.*
> **NGUYÊN TẮC:** *memory càng ngắn gọn, càng hữu dụng; memory càng dài dòng, càng dễ làm AI nhiễu.*

2. SKILLS — ĐỂ AI KHÔNG HỌC LẠI CÙNG MỘT VIỆC MỖI LẦN

Một doanh nghiệp không vận hành bằng cảm hứng. Doanh nghiệp vận hành bằng quy trình.

Hermes đưa logic này vào agent thông qua Skills. Một skill là một tài liệu quy trình có cấu trúc: khi nào dùng, làm từng bước ra sao, lỗi thường gặp là gì, kiểm tra kết quả thế nào. Khi agent hoàn thành một việc phức tạp, kinh nghiệm đó có thể được đóng gói lại thành skill để lần sau không phải mò lại từ đầu.

Điều này biến AI từ "người trả lời" thành "người học quy trình".

> **MINI CASE**
>
> *Lần đầu agent tạo bản tin sáng cho CEO, nó phải học nguồn dữ liệu, format mong muốn, mức độ chi tiết, kênh gửi và cách kiểm chứng. Nếu quy trình đó được lưu thành skill, lần sau CEO chỉ cần nói "làm daily brief", hệ thống có thể đi theo playbook đã chuẩn hóa.*

3. TOOLS — ĐỂ AI CÓ TAY CHÂN, KHÔNG CHỈ CÓ LỜI NÓI

LLM chỉ sinh chữ. Doanh nghiệp cần hành động: đọc file, kiểm tra lịch, gọi API, build website, chạy script, gửi báo cáo, tạo preview, đăng nội dung, kiểm tra đường link, hoặc theo dõi một chỉ số.

Hermes cho agent quyền dùng tool theo cấu hình. Đây là phần biến AI từ người tư vấn thành người thực thi. Nhưng cũng chính vì vậy, quyền dùng tool phải được quản trị nghiêm túc: cái gì được đọc, cái gì được ghi, cái gì cần người duyệt, cái gì phải chạy trong sandbox.

> **RISK BOX**
>
> *AI có công cụ càng mạnh thì quy trình kiểm soát càng quan trọng. Một agent có thể chạy lệnh, gửi email hoặc sửa file không nên được vận hành như một chatbot vui vẻ. Nó cần quyền hạn, vùng cấm, log, approval gate và người chịu trách nhiệm cuối.*

4. ASYNC ORCHESTRATION — ĐỂ AI LÀM VIỆC CẢ KHI BẠN KHÔNG NGỒI CHỜ

Một chatbot thông thường cần bạn mở cửa sổ chat và tiếp tục tương tác. Một AI OS cần làm được việc nền: sáng gửi brief, thứ Sáu tổng hợp pipeline, mỗi ngày theo dõi website, khi có tín hiệu mới thì báo lại.

Hermes hỗ trợ cron jobs và delegation để các tác vụ có thể chạy theo lịch hoặc phân tách thành nhiều luồng độc lập. Đây là điểm rất quan trọng với CEO: AI không chỉ "trả lời khi được hỏi", mà có thể trở thành một lớp vận hành chủ động.

Sơ đồ 2: Một workflow CEO AI OS đơn giản

BƯỚC	VIỆC XẢY RA	VAI TRÒ CỦA HERMES
1	CEO giao mục tiêu	Hiểu intent và ràng buộc
2	Agent đọc memory/skill liên quan	Lấy bối cảnh và quy trình đã học
3	Agent dùng tool cần thiết	Đọc dữ liệu, chạy script, tạo file, kiểm tra link
4	Agent tạo output	Báo cáo, draft, dashboard, preview hoặc task list
5	Agent kiểm chứng	Kiểm tra URL, file, lỗi build, dữ liệu đầu vào
6	Con người duyệt	CEO/team xác nhận trước khi dùng thật
7	Agent cập nhật skill nếu cần	Biến bài học mới thành quy trình tốt hơn

CHƯƠNG 6

06

Component mẫu cho bản full

Decision Box: Khi nào nên dùng Hermes?

TÌNH HUỐNG	NÊN DÙNG HERMES?	LÝ DO
Việc một lần, chỉ cần brainstorm	Có thể chưa cần	Chatbot thường đủ nhanh
Việc lặp lại hàng tuần	Nên cân nhắc	Có thể chuẩn hóa thành skill/cron
Việc cần nhiều công cụ và nhiều bước	Rất phù hợp	Hermes mạnh ở orchestration
Việc đụng dữ liệu nhạy cảm	Chỉ dùng khi có guardrail	Cần phân quyền, sandbox, approval
Việc cần quyết định chiến lược	Dùng như cố vấn, không thay người	AI hỗ trợ phân tích, CEO vẫn chịu trách nhiệm

Checklist: Một workflow tốt để đưa vào AI OS

- Có đầu vào rõ ràng.
- Có kết quả mong muốn rõ ràng.
- Có tiêu chí kiểm tra đúng/sai.
- Có tần suất lặp lại.
- Có người duyệt cuối.
- Có vùng dữ liệu được phép dùng.
- Có quy tắc khi AI không chắc.

NGUYÊN TẮC TRIỂN KHAI

Đừng bắt đầu bằng câu hỏi "AI làm được gì?". Hãy bắt đầu bằng câu hỏi "workflow nào đang làm công ty mất thời gian, lặp lại nhiều, có tiêu chí kiểm tra rõ, và nếu tự động hóa sẽ tạo ROI thật?".

CHƯƠNG 7

07

Ghi chú nguồn research cho bản full

Bản đầy đủ sẽ bám vào các nhóm nguồn sau:

- Tài liệu chính thức Hermes Agent của Nous Research: memory, skills, tools, configuration, security, code execution, gateway.
- Research về AI Operating System và agentic enterprise: vì sao doanh nghiệp cần orchestration thay vì nhiều chatbot rời rạc.
- Các phân tích về persistent memory, skill-based procedural learning, sub-agent delegation, cron automation, MCP/tool gateway và execution sandbox.
- Các giới hạn thực tế: token cost, hallucination, tool failure, bảo mật, quyền duyệt của con người.

Cam kết biên tập: nội dung bản full sẽ viết lại hoàn toàn theo góc nhìn CEO/SME, không copy bản nháp cũ, không biến thành tài liệu kỹ thuật khô, và không pitch CEO AI OS quá đà. CEO AI OS chỉ xuất hiện như ví dụ ứng dụng khi cần.