FDE / DEPLOYMENT CAPITAL / 2026

FDE 真正交付的不是系统

而是“部署资本”

决策 · 语境 · 控制 · 学习 · 经营杠杆

摘要

企业引入 FDE，真正要买的不是一套“能跑”的系统，而是一套能持续做出正确决定、吸收现场语境、守住生产边界并跨场景复用的能力。

这份白皮书从近 90 天的一手信号出发，给出部署资本、双飞轮、决策权架构、双层部署和五个速度等可直接用于立项、治理与复盘的框架。

小红书 | 心晴九天

持续分享 FDE、AI Native 企业与数字化转型实战

免费完整版 · 版本 2026.08 · 核验截止 2026-08-04

欢迎转发用于企业内部讨论，请保留来源

01 / EXECUTIVE THESIS

FDE 是一套部署操作系统

职位只是载体，组织能否持续形成结果才是重点。

最短结论

部分建造工作正在被 Agent 化，头部厂商却同时加码嵌入式部署。两件事并不矛盾：工程执行变快以后，真正稀缺的能力转向目标、语境、决策权、控制、采用与产品学习。

因此，我更愿意把 FDE 理解为一套跨越客户与供应方的部署操作系统。它当然包含工程建设，但不止于工程建设。它要回答：什么值得做，谁能拍板，Agent 可以做到哪一步，什么证据足以上线，以及现场经验怎样进入下一次部署。

如果项目只留下代码和接口，客户仍然依赖原团队解释规则、处理异常和推动采用，那么系统虽然上线，组织能力并没有真正留下。本文把那些可以被客户拥有、被团队复用、被治理机制约束的能力，统称为“部署资本”。

阅读时请区分三类内容：事实来自一手公开资料；咨询机构观点作为外部参照；“部署资本”“双飞轮”“五个速度”等为本文框架，不冒充官方定义。

02 / MARKET SIGNAL

部署能力在加码，建造工作正在 Agent 化

01 OpenAI：把部署能力放进公司级投资

5 月 11 日，OpenAI 宣布 Deployment Company，并披露超过 40 亿美元的初始投资。拟议收购完成后，预计带来约 150 名部署人才，并与 19 家伙伴协作。交易仍取决于交割条件，不能把规划写成已经完成。

02 Anthropic × DXC：把 FDE 培训推向规模化

6 月 11 日，双方宣布面向受监管系统的 FDE 认证计划，目标是培训数万名人员。这里的“数万名”是计划目标，不是已完成人数。

03 Palantir：Agent 开始覆盖更多建造环节

AI FDE 与 MCP 等能力覆盖数据、Ontology、Functions、应用、治理检查和依赖理解，但变更仍受权限、分支、审查和生产责任约束。

本文判断

FDE 没有消失，部署责任正在重新分配：Agent 承担更多生成、连接、测试、调试与依赖理解；人类守住构建审查、生产责任、目标、权责、风险、采用和产品化。

03 / COST MIGRATION

工程环节更快，部署未必更轻

当编码、集成和测试的部分环节提速，部署成本不会凭空消失，而会更快暴露在过去容易被工程工作掩盖的地方。

01	语境熵	规则散在人的经验、群聊、文档、系统和例外里。模型看见材料，不等于理解企业如何做决定。
02	决策延迟	流程、数据、风险和收益由不同部门掌握。没有明确拍板人，技术团队只能等待或替业务猜。
03	控制复杂度	Agent 能行动后，身份、权限、Eval、审计、升级、回滚和变更管理都必须进入运行时。
04	变革容量	生产系统会改变岗位、流程和激励。能上线，不等于一线愿意把真实工作交给新系统。

真正的成本迁移

工程产能越容易获得，组织越需要把隐性语境和分散权力变成可执行、可追责、可迭代的系统。FDE 的价值因此不是“多写一点代码”，而是缩短从问题到证据、从证据到决策、从决策到采用的距离。

04 / DEPLOYMENT CAPITAL

什么是“部署资本”？

本文定义

部署资本，是一次部署留下的、客户可以继续拥有和复用的决策、语境、控制与学习资产。它是组织能力框架，不是会计准则中的资本化结论。

系统上线是一场事件。部署资本回答的是：项目离场以后，企业是否更会选场景、更懂自己的业务语义、更能安全运行 Agent，也更能把现场反馈转化成产品与流程改进。

判断有没有形成资本，可以追问三个问题。第一，这项能力是否已经从个人经验变成组织可访问的资产？第二，客户是否能在没有原 FDE 的情况下继续运行和修改？第三，第二个场景是否真的少走了旧路？

只要答案仍然依赖“找那个最懂的人”，留下的就不是资本，而是新的关键人风险。真正危险的不是第一次部署贵，而是每次部署都同样贵。

05 / DECISION CAPITAL

先把战略意图变成可执行的决定

很多 AI 项目不是做不出来，而是从未把关键决定写清楚：要改变哪个经营结果，什么叫成功，谁有权缩范围、暂停或回滚，哪些例外必须交给人。

01	价值树	把经营结果拆成可观测的驱动因素，避免团队只对功能清单负责。
02	基线	记录不做项目时的真实表现、数据口径和观察窗口，否则上线后无法归因。
03	决策权	明确谁能选、批、停、升级和回滚，让争议在建设前被处理。
04	停止条件	事先约定假设被证伪或风险过高时如何结束，防止项目只进不退。

常见失败

只有项目经理，没有业务结果 Owner；只有路线图，没有停止条件；所有争议都留到上线前。这样的团队即使技术完成，也没有真正的部署决策能力。

06 / CONTEXT CAPITAL

模型读过文档，不等于企业拥有了语境

企业语境不是文档数量，而是业务世界里稳定存在的对象、关系、状态、规则、例外和证据。FDE 的工作不是把更多材料塞进上下文窗口，而是持续降低业务语义的不确定性。

01	对象与关系	客户、订单、设备、案件、任务分别是什么；谁属于谁、依赖谁、影响谁。
02	状态与规则	对象处在哪个阶段、何时迁移；正常路径、阈值、优先级和约束是什么。
03	例外与证据	缺数、冲突、拒绝和边界工况如何升级；每个判断能否追溯到来源和版本。

语境资本必须能进入系统：对象有主键，状态有迁移条件，规则有版本，证据有来源，例外有责任人。只写在 prompt 里的知识，通常还没有成为企业资产。

语境债务

当规则只存在于少数人的经验、临时群聊和口头补充里，每新增一个 Agent，都会放大不一致。

07 / CONTROL CAPITAL

治理必须进入 Agent 的运行时

传统治理常发生在上线前：评审一次、签字一次、发布一次。Agent 会持续调用工具、读取数据、改变状态，因此控制机制必须跟着每一次行动运行。

01	身份与权限	每个 Agent 有明确身份和责任域，按任务取得最小权限，敏感动作需要再次批准。
02	分层 Eval	离线评正确性，模拟评工具轨迹，在线评延迟和接管，业务层评行为与结果。
03	审计与升级	输入、输出、工具、版本和理由可追溯；低置信、冲突或越权时自动转人工。
04	回滚与变更	模型、规则、数据和流程都有版本，异常时能恢复，并知道由谁决定恢复。

生产红线

如果高影响动作的控制方案仍是“让模型自己判断”，默认不应进入生产。

08 / LEARNING CAPITAL

现场信号必须能够改变产品

FDE 最独特的价值，不是更接近客户，而是把现场异常变成产品学习。没有进入路线图和跨场景验证的经验，最终只会留在个人脑中。

01	记录异常	保留真实失败、输入、环境和后果，不用一句“用户问题”带过。
02	识别模式	区分客户配置、行业共性和平台缺口，明确哪些差异值得产品化。
03	沉淀资产	把模式变成组件、连接器、Eval、Ontology、策略或 playbook。
04	跨场景验证	在第二个部署里验证资产是否减少了人天、风险或等待。

判断标准

如果第二个客户仍从零开始，或者每次离场都要继续找同一个人，这不是学习资本，只是项目经验。

09 / DUAL FLYWHEEL

合格的 FDE 必须同时转动两个飞轮

经营飞轮

价值假设 → 工作流重构 → 生产采用 → 行为改变 → 指标变化 → 继续投资

经营飞轮要求项目离开 Demo，进入真实业务节奏。它关心的不是“功能完成多少”，而是谁真的改变了工作方式，以及这个变化是否推动了经营指标。

产品飞轮

现场例外 → 可复用模式 → 组件 / Eval / Ontology → 第二次部署 → 反馈验证

产品飞轮要求供应方拒绝无限定制，把现场差异压回平台。一次部署可以例外，第二次仍然例外，就说明团队还没有形成复用能力。

为什么必须两边一起转

只转经营飞轮，FDE 会退化成高质量定制；只转产品飞轮，团队会拥有漂亮架构，却停在实验室。FDE 的独特价值，是让客户结果与产品进化互相供能。

10 / DECISION RIGHTS

Pod 的本质不是人头，而是决策权

FDE Pod 可以有不同岗位组合，但五类决定不能悬空。岗位可以合并，责任不能被“共同负责”稀释。

关键决定	最终主责	共同参与
什么结果值得做	客户业务 Owner	财务、运营、FDE / TDL
范围、路径与验收	TDL / 交付负责人	FDE、客户技术与业务
Agent 能看什么、做什么	业务 + 数据 + 安全 / 合规	平台、FDE、服务 Owner
上线、暂停与回滚	生产服务 Owner	业务、风险、FDE
哪些能力进入产品	产品 / 研究 + FDE	客户 Owner、平台团队

两条铁律

没人有权“停”，项目会无限实施；没人有权“标准化”，团队会无限定制。

11 / JOINT OPERATING MODEL

供应方不能替客户拥有结果

供应方可以负责构建和方法，但业务结果必须由客户内部的 Owner 拥有。否则项目会产生一个危险错觉：供应商越努力，客户越依赖；交付越成功，移交反而越难。

01 客户业务 Owner

定义价值、开放真实流程、推动采用并签收结果。没有这个角色，项目只能优化技术产出。

02 客户技术、数据与风险团队

承担系统边界、数据责任、权限批准和运行保障。FDE 不能绕过这些控制面。

03 TDL、FDE、产品与研究

把目标变成路径和生产系统，再把现场模式压回平台、组件和路线图。

移交也不应等到最后一周。更合理的路径是：旁观 → 共建 → 客户主导、FDE 辅助 → 客户独立运营。每一步都需要权限、运行手册、应急演练和能力验收。

真正的完成

不是供应方把系统交出去，而是客户有能力接住决策、运行和改进责任。

12 / CHINA OPERATING MODEL

中国大型组织，更适合双层部署

大型组织通常同时面对两种需求：总部需要统一控制模型、权限、数据和供应商；业务一线又必须在真实环境里处理例外、验证价值并推动采用。把两者揉成一个中央团队，往往既慢又离现场太远。

01 **中央控制层**

负责平台与模型准入、身份权限、数据安全、Eval、审计、观测、采购标准，以及跨场景复用资产和产品路线图。

02 **场景部署单元**

由用户单位、业务 Owner、真实环境和一线流程组成，负责价值目标、异常工况、验证报告、常态运营、升级与回滚。

两层之间不是汇报关系，而是一份联合体契约：谁牵头、谁开放场景、谁提供数据、谁签收结果、哪些能力进入公共资产、重大风险如何升级。

中国政策实践给出的启发

2026 年 6 7 月，工信部、国资委与地方“AI+”实践进一步强调场景开放、用户单位参与、验证机制和协同攻关。本文借鉴的是组织逻辑，不把具体试点写成通用 FDE 标准。

13 / JOINT CONTRACT

合同不是采购收尾，而是部署操作系统

复杂部署的失败，常常不是因为技术条款不够多，而是关键协作关系没有提前写清。至少要在立项前确认以下六件事。

01	场景与目标	谁是用户单位，真实环境在哪里，基线和验收由谁签字。
02	数据责任	数据由谁提供、允许做什么、质量谁负责、退出时怎样处理。
03	任务边界	供应方必须交付什么，客户必须提供什么，哪些问题不属于驻场团队。
04	知识产权	通用能力、行业模式和客户专有逻辑如何区分，哪些资产可以复用。
05	变更与退出	模型升级、重大风险、回滚、暂停和终止由谁决定。
06	利益机制	按人天、里程碑、结果还是复用收益付费，会把团队激励到哪个方向。

契约设计决定了团队最终会优化“项目收入”，还是优化“客户结果与复用能力”。

14 / PORTFOLIO MATRIX

什么场景值得上重 FDE？

不是所有 AI 项目都需要重部署。先看业务价值，再看语境熵：例外多不多、跨部门多不多、决策是否依赖隐性经验、错误后果是否高。

场景	推荐模式	原因
高价值 × 高语境熵	重 FDE	规则、例外、控制与采用必须一起进入系统
高价值 × 低语境熵	标准平台 + 轻部署	成熟能力不应重复消耗昂贵驻场人力
低价值 × 高语境熵	先诊断，不急着建	很可能是组织问题，未必是 AI 机会
低价值 × 低语境熵	直接买工具 / 自动化	不要把小题做成转型工程

组合管理，而不是单点立项

重 FDE 场景应该少而关键，用于建立生产证据和学习资产；低语境熵场景则尽量产品化。否则组织会把最贵的人困在最容易标准化的工作里。

15 / VALUE CASE

ROI 不是一张表，而是一条因果链

上线后指标变好，不等于 AI 导致。一个可信的价值案例，必须把技术动作与经营结果之间的因果链写清。

01	结果	先定义收入、成本、周期、质量或风险中哪一项必须改变。
02	行为	指出哪个关键岗位、哪一个真实动作需要发生变化。
03	工作流	写清输入、判断、动作、反馈与异常如何重构。
04	AI 贡献	区分 Agent 自动完成、建议、人审和禁止自动化的步骤。
05	约束	把数据、权限、合规、系统容量和人工接管纳入模型。
06	证据	记录基线、领先指标、结果指标，以及同期其他变化。

不要把相关性当归因

条件允许时采用分组、分期或历史对照；至少也要记录流程、人员、季节性和其他项目变化。价值案例必须经得住财务与业务 Owner 的追问。

16 / EVAL & CONTROL

没有分层 Eval，就没有可控迭代

不同层级回答不同问题。把所有评估压成一个总分，会掩盖最危险的失败模式。

层级	评什么	最低产物
离线	正确、完整、引用、拒答、鲁棒	真实样本集、标注与阈值
模拟	工具调用、权限、异常、升级、回滚	场景脚本、预期轨迹、失败注入
在线	延迟、成本、接管、漂移、事故	监控、告警、审计日志
业务	行为和经营结果是否改善	基线对照、Owner 签收

上线门禁

样本来源、成功阈值、严重错误、人工批准点、停止条件、回滚方式、签字人和观察窗口必须同时存在。不能用 Demo 样本验收生产系统，也不能让模型自己给自己打分后直接上线。

17 / ADOPTION & TRANSFER

真正的采用，是责任和工作方式发生变化

使用次数不等于采用。真正的采用发生在组织把日常决策、运行责任和异常处理交给新工作流，并且知道什么时候必须接管。

01 **旁观**

关键用户能复述新流程、边界和风险；FDE 收集异议，不急着把培训当作完成。

02 **共建**

客户参与规则、例外和 Eval，用真实样本共同决定系统应该如何行动。

03 **客户主导**

客户运行日常工作流，FDE 旁站修正；用 SLA、接管率和事故演练证明能力。

04 **独立运营**

客户维护规则、监控和回滚，供应方只处理产品级问题。

移交失败的信号

只有 FDE 能改规则；客户不知道何时升级；监控只由供应商查看；事故仍靠群里叫人。这样的“采用”只是供应商代运营。

18 / FIVE SPEEDS

别只看 ROI，更要看五个速度

单次 ROI 只能解释项目值不值得做，无法解释组织有没有变得更会部署。五个速度更能暴露系统性瓶颈。

01	证据速度	从立项到第一个足以改变决策的生产证据。
02	稳定速度	从原型到可持续运行、可监控、可回滚。
03	闭环速度	从发现例外到修正规则、Eval 或流程。
04	移交速度	客户从旁观、共建走到独立运营。
05	复用速度	第二个场景少走了多少旧路。

本文不设置伪精确行业公式，只看方向：业务价值持续上升，同时新增部署的边际人天、风险与等待时间持续下降。

> ### 部署杠杆
>
> 下一次更快，不是因为团队更拼，而是因为决策、语境、控制和学习资产已经留下。

19 / ECONOMICS

不要只算项目毛利，要看两张损益表

01 部署损益表

记录本次价值与收入、FDE 与客户投入、集成和变更成本、运行支持成本，以及失败与风险准备。它回答“这次项目是否值得”。

02 学习损益表

记录新增可复用资产、第二次部署节省的人天、更快成交与验收、路线图影响，以及资产维护成本。它回答“这次项目有没有让未来更轻”。

早期高不确定项目可能项目毛利不漂亮，却产生高价值的平台学习。但如果每个项目都用“这是研发”解释亏损，又没有跨部署复用证据，那只是在掩盖服务业务。

学习必须被资产和下一次部署验证：什么被复用、节省了多少等待、减少了哪些风险、是否缩短了验收。如果这些问题没有答案，就不能把亏损自动解释成投资。

最终判断

一次部署贵并不可怕；可怕的是组织永远不知道为什么贵，而且每次都同样贵。

20 / 90-DAY ROADMAP

用 90 天建立证据、控制与复用

这是本文管理 timebox，不是行业统一周期。

0–30 建立证据

选择高价值、高语境熵场景；确认业务 Owner、基线和停止条件；画出对象、状态、例外与决策权；冻结最小生产证据窗口。

31–60 进入受控生产

打通最小端到端工作流；建立身份、权限、Eval 与审计；小流量上线并记录接管、异常与成本；每周明确扩、改或停。

61–90 形成部署资本

让客户主导日常运营；沉淀组件、Eval、Ontology 与 playbook；在第二个场景验证复用；比较五个速度与边际人天。

高监管或复杂采购场景应按审批与验证周期调整，不要为追求“90 天上线”跳过必要控制。时间盒的作用，是逼迫团队持续产生决策证据，而不是制造虚假速度。

90 天最低验收

至少一个生产场景；客户可独立运营；四类部署资本可见；一项资产在第二场景复用；重大风险有批准、日志、演练与回滚证据。

21 / WEEKLY REVIEW

30 分钟周会，只看证据和决策

FDE 周会不应该变成开发进度播报。每五分钟只回答一个问题，并带来可以检查的证据。

01	价值	基线、领先指标和业务结果发生了什么变化。
02	采用	谁在用、谁没用、哪些关键动作仍然依赖人工。
03	异常	最高频失败、接管、越权和事故分别是什么。
04	资本	本周新增了哪项决策、语境、控制或学习资产。
05	杠杆	五个速度是否改善，第二场景复用了什么。
06	决策	扩、改还是停；由谁负责，何时回来验收。

三个红旗

“整体进展顺利”——请给数字；“用户反馈不错”——请给行为证据；“再给两周就好”——请说明哪个假设被证伪、谁拍板继续。

22 / SOURCES · 1/2

来源与可说边界

事件按发布日期；岗位与产品页为截至 8 月 4 日的当前快照。点击条目可跳转原文。

O1 OpenAI Deployment Company 2026-05-11

openai.com/index/openai-launches-the-deployment-company

O2 OpenAI Forward Deployed Engineer 截至 2026-08-04

openai.com/careers/forward-deployed-engineer-%28fde%29-sf-san-francisco

O3 OpenAI Technical Deployment Lead 截至 2026-08-04

openai.com/careers/technical-deployment-lead-forward-deployed-engineering-%28fde%29-nyc-new-york-city

O4 OpenAI Frontier 截至 2026-08-04

openai.com/business/frontier

P1 Palantir AI FDE 当前产品页

www.palantir.com/docs/foundry/ai-fde/overview

P2 Palantir MCP GA 2026-06-25

www.palantir.com/docs/foundry/announcements/2026-06

P3 Palantir Workflow Lineage 2026-07-23

www.palantir.com/docs/foundry/announcements

22 / SOURCES · 2/2

来源与可说边界

事件按发布日期；岗位与产品页为截至 8 月 4 日的当前快照。点击条目可跳转原文。

A1 Anthropic × DXC alliance 2026-06-11

www.anthropic.com/news/dxc-anthropic-alliance

C1 工信部 / 国资委：具身智能实景实训 2026-06-08

wap.miit.gov.cn/jgsj/kjs/wjfb/art/2026/art_cd666691abf8471fb8553d463aa416e3.html

C2 国资委：央企高价值场景 2026-07-27

wap.sasac.gov.cn/n2588020/n2588072/n2590902/n2590904/c35690985/content.html

C3 深圳：AI+ 联合攻关 2026-06-11

www.sz.gov.cn/cn/xxgk/zfxxgj/tzgg/content/post_12838491.html

S1 BCG：Agentic AI 团队转型 2026-06-19

www.bcg.com/publications/2026/agentic-ai-turns-every-team-into-its-own-transformation-engine

S2 BCG：受监管行业 Agent 平台 2026-07-20

www.bcg.com/publications/2026/building-enterprise-ai-agents-in-regulated-industries

S3 McKinsey：Agentic 软件交付 2026-05-28

www.mckinsey.com/capabilities/mckinsey-technology/our-insights/rewiring-software-delivery-for-the-agentic-era

使用说明 | 小红书：心晴九天

“部署资本”“双飞轮”“五个速度”“双层部署”是本文框架，不是厂商或政策官方标准；完整边界见证据映射。欢迎关注「心晴九天」，继续交流 FDE 与 AI 转型实战。