



Vaysen Trade CRM

开源项目功能白皮书

面向外贸企业的客户经营、沟通、报价、订单、分析与 AI 协同工作系统

68 天

完整开发周期*

>100 亿 Token

多轮开发与审计*

>24 小时

最长单任务*

70 / 38 / 15

页面 / 后端模块 / 迁移

* 68 天、Token 与最长任务为项目负责人提供的完整项目周期统计；代码树计数来自 2026-07-17 快照。

公开预览版 0.9 · 文档日期 2026-07-17 · 所有界面截图均使用虚构演示数据

公开版说明与证据边界

这份白皮书用于开源前介绍产品，不是销售承诺、合规认证或生产部署保证。

隐私保护

原系统来自真实企业定制项目。公开文档不写入客户名称、域名、邮箱、账号、服务器、密钥、实际联系人和真实业务记录。所有截图通过真实前端运行时接入虚构演示 API 后重新拍摄。

功能状态分层

已验证：代码、路由、界面或验收证据可确认。Beta：功能存在但仍需部署/边界复核。开发中：当前任务正在实现，不能当成已交付。暂不开放：明确隐藏或禁止。

标记	在本文中的含义	读者应如何理解
READY	当前版本已有可核验能力	仍需按自己的环境完成配置、迁移与验收
BETA	页面/模块存在，但集成或生产边界仍在收口	建议先在隔离环境做小范围试用
BUILDING	代码正在开发或等待验收	只作为路线图，不纳入当前可用清单
DISABLED	出于安全、合规或成熟度原因暂不开放	不要绕过开关或权限边界

截图说明

真实截图指真实项目页面、组件、导航、状态逻辑与交互结构；数据为公开虚构样本。AI 页面显示的“执行内核未连接/状态未知”是演示环境没有连接真实外部执行器时的 fail-closed 表现。

目录

按“业务问题 - 工作流程 - 模块能力 - 技术与开源”展开。

01 产品与开发背景

定位、目标用户、68 天开发过程、设计原则

02 客户经营与获客

客户资产、看板、360 档案、时间线、导入查重与评分

03 沟通、报价与订单

邮件、WhatsApp、报价/PI、订单交付、产品与素材

04 AI 业务助理

工作简报、客户检索、背调、报价准备、权限与审计

05 分析与管理

邮件指标、客户阶段、团队绩效、经营驾驶舱

06 工程与安全

架构、数据、认证、密钥、AI 沙箱、部署、备份与验收

07 开源准备

License 状态、脱敏、安装、贡献、落地方法与模块清单

一句话：把外贸业务过程变成可追踪、可协作、可复盘的系统

它不是只存联系人，也不是让 AI 替人拍板；核心是统一业务事实、固化动作、保留证据。

客户资产

READY

联系人、可信联系方式、来源、阶段、等级、标签、负责人和历史动态归一。

渠道沟通

READY / BETA

邮件工作台、群邮监控、WhatsApp 工作区与客户档案互相联动。

交易交付

READY / BETA

报价单、PI、样品单、合同草稿与订单阶段进入同一业务链。

AI 协同

READY

读取真实 CRM 数据，生成简报、检索客户、创建背调任务、准备报价 PDF。

管理分析

READY

客户漏斗、邮件趋势、团队表现、异常和失联风险形成经营视图。

安全与运维

READY / EVOLVING

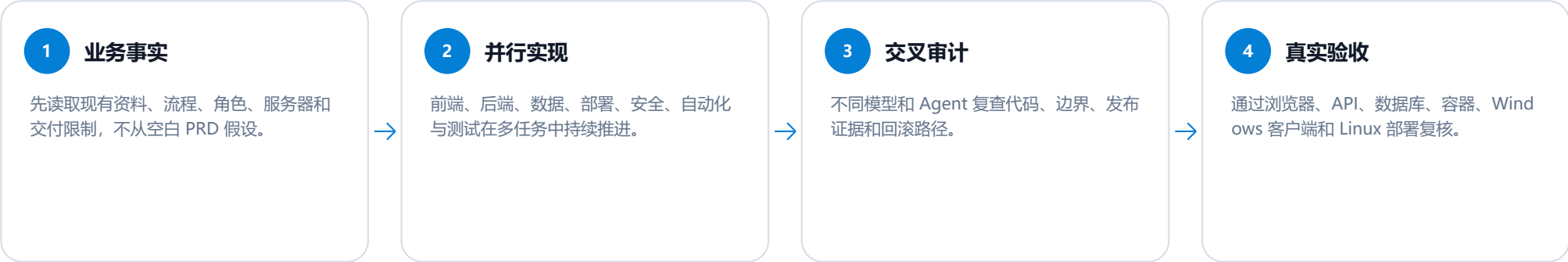
多租户、RBAC、短令牌、密钥加密、队列、备份、容器隔离与 fail-closed。

企业最终得到什么

不是另一套需要业务员重复录入的工具，而是一条从“发现客户 - 验证 - 沟通 - 报价 - 跟进 - 成交 - 交付 - 复盘”贯通的数据链。老板能看见真实过程，业务员能减少翻聊天记录和表格，AI 只能在授权范围内加速重复工作。

68 天开发不是堆页面，而是连续把业务风险写进系统

项目由真实企业场景推动，经过 Claude 与 GPT-5.6 多 Agent 多轮开发、审计、修复和验收。



指标	来源	正确解读
68 天开发周期	项目负责人提供	覆盖完整对话与多轮开发，不等于当前 Git 目录的首个提交时间
>100 亿 Token	项目负责人提供	包含探索、实现、审计、复测和长任务，不代表模型输出都进入代码
>24 小时最长单任务	项目负责人提供	体现持续验收与问题收敛，不应被当作效率 KPI
70 页面 / 38 模块 / 15 迁移	2026-07-17 代码树	是结构计数，不等于 70 个页面全部已达到同一成熟度

为什么必须区分统计来源

公开项目最怕把“过程投入”包装成“质量证明”。真正的质量仍要由可复现构建、测试、迁移、部署、权限审计和用户使用结果来证明。

外贸团队最常见的不是“没有 CRM”，而是业务事实分散

系统针对日常工作里最容易丢失、重复、失控的环节设计。

客户散落

Excel、邮箱、WhatsApp、平台询盘和个人记忆各自一份，无法确定最新状态。

身份不可信

同名、号码尾号、不同邮箱容易误合并，造成串客、错发或报价对象错误。

跟进靠记忆

报价后无人提醒、客户长期失联、业务员离职后历史无法接续。

沟通无证据

邮件、聊天、附件、报价版本和客户承诺没有统一时间线。

报价与订单断开

价格、产品、规格、PI、生产、质检、出货和回款各自维护。

AI 权限过大

把通用 Agent 直接接数据库、Shell、渠道发送，速度提高但风险不可控。

产品判断

先统一事实和责任，再谈自动化。任何 AI 动作都必须落回 CRM 记录、权限、审批和可追溯回执；否则只是把零散的人工错误放大成高速的自动错误。

六条产品原则

这些原则决定了功能取舍，也决定开源后什么可以扩展、什么不能绕过。

原则	系统行为	企业价值
业务事实优先	客户、沟通、报价、订单和任务以数据库记录为准	减少多人各执一词
可信身份优先	邮箱/电话/WhatsApp 完整号码作为身份锚点，不凭相似姓名合并	降低串客和错发
人工判断保留	价格、承诺、发送、删除、权限和部署必须经过人	让责任边界清晰
默认失败关闭	状态不明、授权缺失、目标不唯一时拒绝执行	避免“猜着做”
过程可追溯	动作写入 run、receipt、audit log、timeline 或版本记录	可复盘、可审计
渐进式自动化	先读、再准备、后审批；最后才考虑受控执行	用小风险验证自动化收益

开源扩展建议

新增渠道或 Agent 工具时，优先复用“租户 - 角色 - 能力 - 授权 - 幂等 - 回执”链路，而不是在前端按钮里直接调用外部 API。

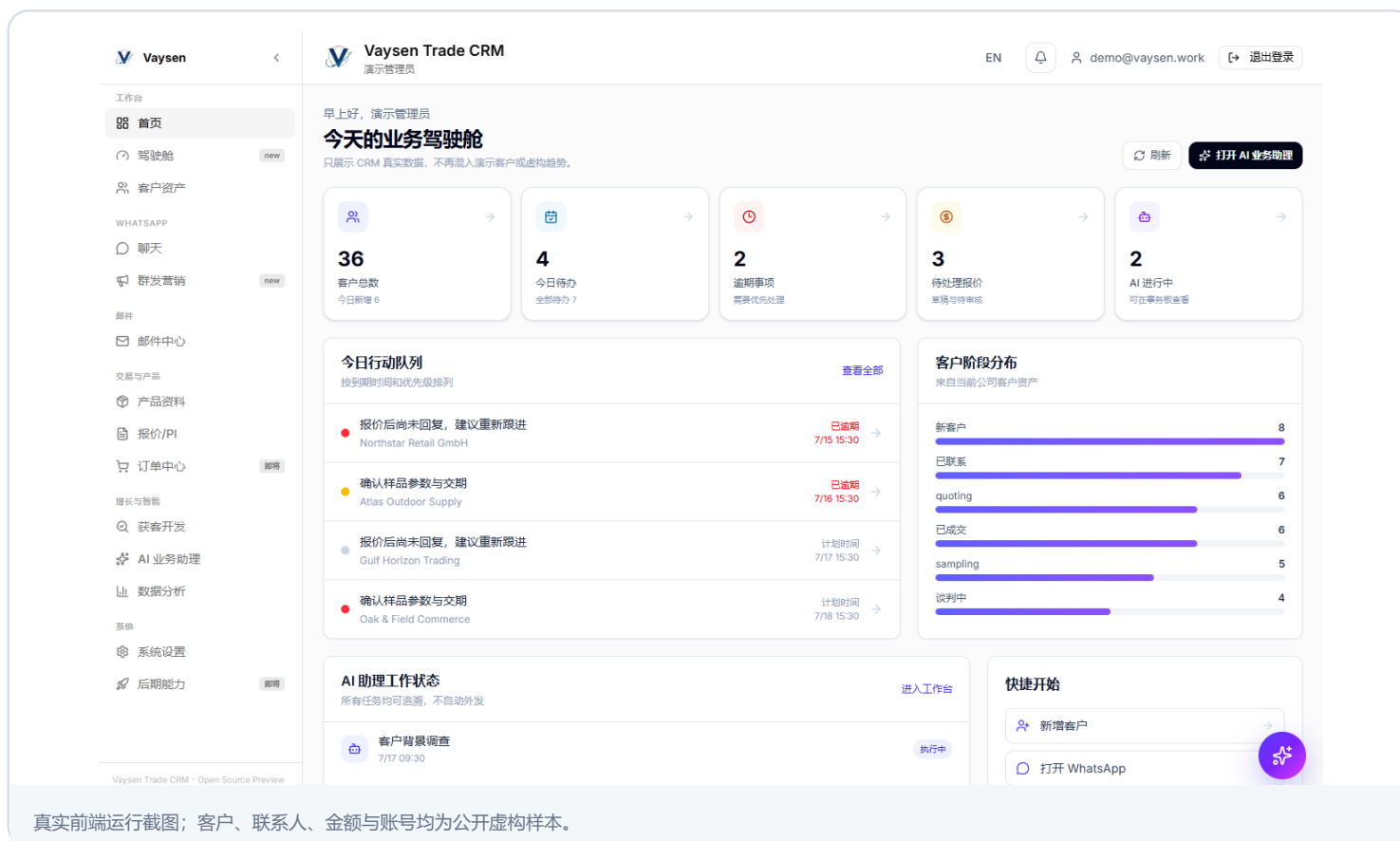
功能地图与成熟度

同一个仓库里既有成熟主链，也有 Beta 和正在开发的能力。

业务域	核心能力	状态	说明
客户资产	客户/联系人/标签/等级/阶段/负责人/导入导出/查重	READY	主数据主链
获客与邮件	线索池、邮箱验证、AI 草稿、队列、打开/点击/回复/退信	READY	需合法来源与发信配置
WhatsApp	会话工作区、客户关联、广播入口、报价附件准备	READY/BETA	依赖外部渠道账号
报价与订单	报价/PI/合同/样品单、版本、订单阶段、回款	READY/BETA	订单入口仍标记“即将”
产品与素材	产品资料、类别、规格、素材、定制器	BETA	不同部署可按业务裁剪
AI 业务助理	简报、检索、背调任务、报价 PDF 准备	READY	自动外发仍关闭
主管执行模式	临时授权、审批中心、受控写入与外发	BUILDING	TASK-117 正在实现
微信负责人通道	扫码绑定、唯一 owner 指令、回执验收	BETA	真机验收尚未闭环
AI 语音客服	语音相关代码与页面	DISABLED	当前发布隐藏

首页业务驾驶舱

把客户、待办、逾期、报价、AI 任务和阶段分布集中到一天的工作入口。



落地能力

- 真实数据驱动的客户总数、今日待办、逾期、待报价与 AI 进行中指标。
- 按时间和优先级展示今日行动队列，业务员可直接进入客户或任务。
- 客户阶段分布、快捷动作和 AI 工作状态不再依赖人工周报。
- 演示数据使用 36 个虚构客户；生产部署应按角色过滤数据范围。

企业帮助

把页面动作写回业务事实，减少跨表查找、口头交接和重复确认；数据是否带来结果仍取决于流程执行与团队纪律。

业务员的一天：从队列开始，而不是从聊天列表开始

系统先告诉人“今天该处理什么”，再把动作回写到客户和交易记录。



角色	关注页面	判断标准
业务员	首页、客户资产、沟通、报价、跟进	每个重点客户都有清晰下一动作
销售经理	驾驶舱、数据分析、团队队列	客户分配、超期、漏斗和发送质量可见
老板	经营驾驶舱、异常、成交与回款	看真实业务变化，不依赖人工汇总报表

关键要求

使用 CRM 的最低标准不是“每天登录”，而是重要客户、重要沟通、重要报价和下一步必须进入系统；否则再强的 AI 也只能读取残缺事实。

客户资产中心：列表视图

把客户从“联系人表格”升级为带阶段、等级、标签、负责人、最近联系和来源的业务资产。

Vaysen

Vaysen Trade CRM

EN

demo@vaysen.work

退出登录

工作台

首页

驾驶舱

客户资产

WHATSAPP

聊天

群发营销

邮件

邮件中心

交易与产品

产品资料

报价/PI

订单中心

增长与智能

获客开发

AI 业务助理

数据分析

系统

系统设置

后期能力

客户资产中心

所有客户、联系人、沟通记录、询盘、报价和订单统一管理

列表

看板

导入

新增客户

客户阶段

动态客群

搜索公司名称、联系人...

全部等级

全部来源

全部状态

共 36 个客户

公司名称	客户标签	客户阶段	主要联系人	最新动态	跟进人	最近联系	国家/地区	来源
Northstar Retail GmbH	A级 重点跟进	新客户	Anna Keller +1 202 5...	最新动态	Leo	刚刚	德国	网站询盘
Atlas Outdoor Supply	B级 独立站客户	已联系	Michael Reed +1 20...	最新动态	Mia	22小时前	美国	阿里询盘
Gulf Horizon Trading	B级 展会客户	样品中	Omar Hassan +1 20...	最新动态	Leo	1天前	阿联酋	获客开发
Brightline Market Group	A级 展会客户	样品中	Omar Hassan +1 20...	最新动态	Leo	2026/7/9	德国	获客开发
Maple Harbor Brands	B级 独立站客户	谈判中	Sophie Martin +1 20...	最新动态	Leo	4天前	德国	Google
Northstar Retail GmbH	C级 重点跟进	新客户	Anna Keller +1 202 5...	最新动态	Leo	1天前	德国	网站询盘
Brightline Market Group	B级 展会客户	样品中	Omar Hassan +1 20...	最新动态	Leo	2026/7/7	德国	获客开发
Summit Consumer Goods	C级 重点跟进	报价中	Emily Brown +1 202 ...	最新动态	Mia	2026/7/8	美国	WhatsApp
Southern Cross Imports	B级 展会客户	已完成	Liam Wilson +1 202 ...	最新动态	Mia	5天前	美国	展会
Atlas Outdoor Supply	A级 独立站客户	已联系	Michael Reed +1 20...	最新动态	Mia	2天前	美国	阿里询盘
Summit Consumer Goods	A级 重点跟进	报价中	Emily Brown +1 202 ...	最新动态	Mia	刚刚	美国	WhatsApp
Bluewave Sourcing	A级 独立站客户	谈判中	Sophie Martin +1 20...	最新动态	Leo	2026/7/7	阿联酋	Google
Delta Homeware BV	A级 重点跟进	新客户	Anna Keller +1 202 5...	最新动态	Leo	6天前	阿联酋	网站询盘
Gulf Horizon Trading	B级 展会客户	样品中	Omar Hassan +1 20...	最新动态	Leo	3天前	阿联酋	获客开发
Bluewave Sourcing	C级 独立站客户	谈判中	Sophie Martin +1 20...	最新动态	Leo	19小时前	阿联酋	Goog
Oak & Field Commerce	A级 重点跟进	报价中	Emily Brown +1 202 ...	最新动态	Mia	2天前	英国	WhatsApp

列表使用公开演示 API；邮箱为 example.com，占位电话不对应真实客户。

落地能力

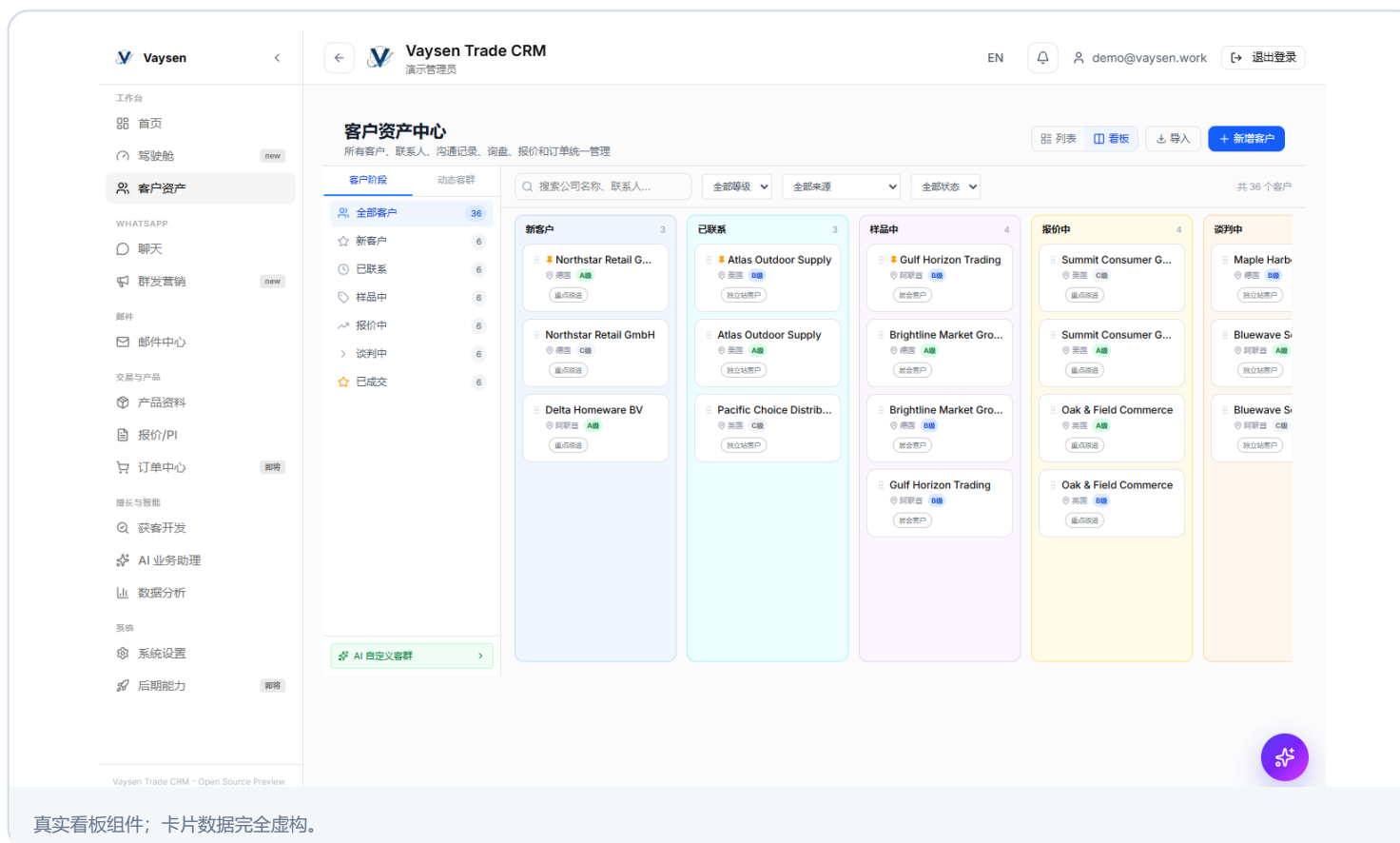
- 按阶段、等级、来源和状态筛选；支持公司名、联系人和邮箱搜索。
- 列表中直接看到主要联系人、跟进人、最近联系、国家和来源。
- 支持批量选择、状态更新、负责人调整、标签、导入与导出。
- 客户身份、沟通、报价和订单可以从同一行进入。

企业帮助

把页面动作写回业务事实，减少跨表查找、口头交接和重复确认；数据是否带来结果仍取决于流程执行与团队纪律。

客户资产中心：阶段看板

用流程阶段观察工作量和卡点，而不是只看客户数量。



落地能力

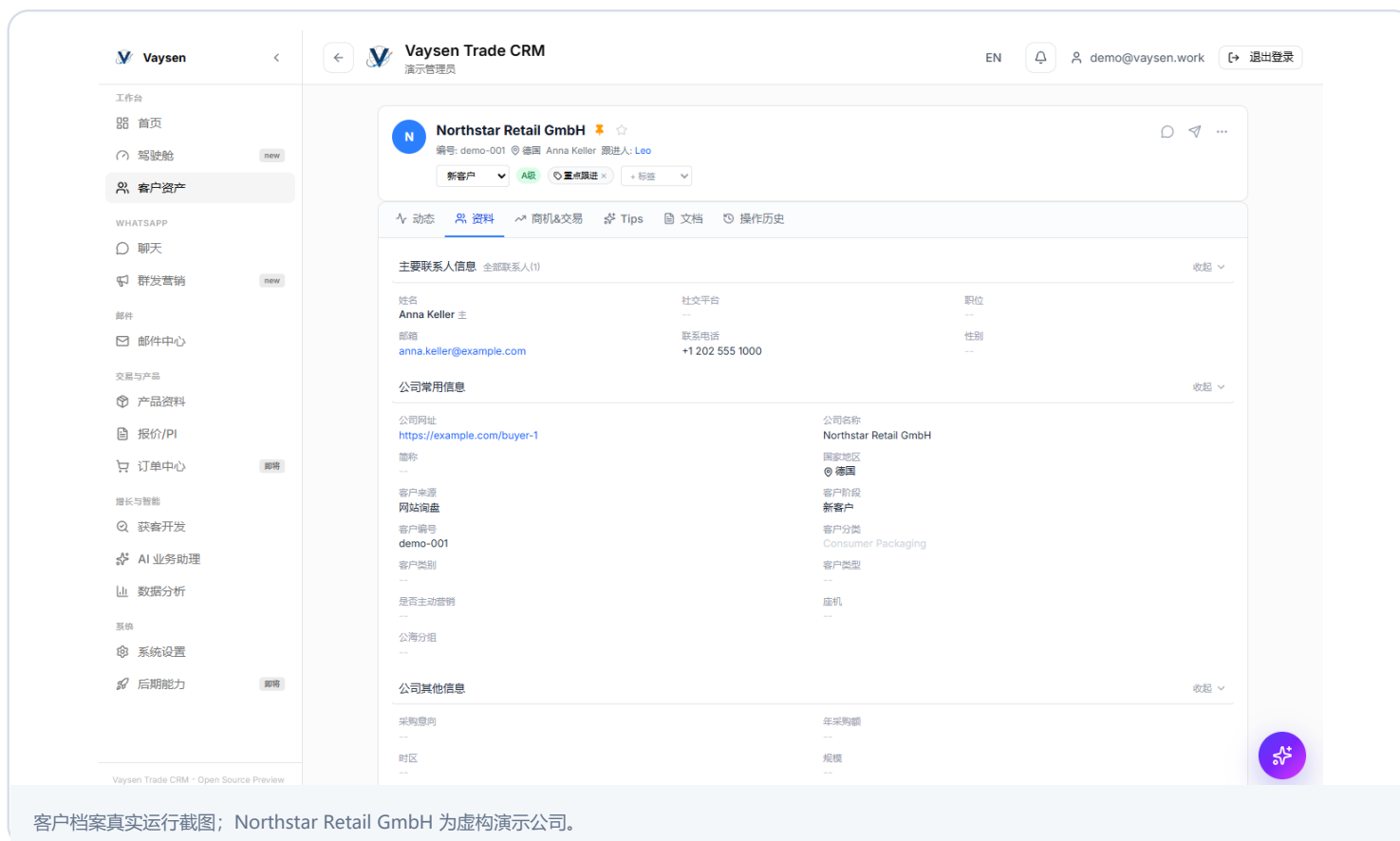
- 新客户、已联系、样品中、报价中、谈判中、已成交等阶段并列。
- 卡片显示客户、国家、等级和标签；高价值客户可固定关注。
- 适合销售例会检查阶段拥堵、无人跟进和长期停留。
- 阶段变化应由真实业务事件或人工判断触发，不能只凭 AI 猜测。

企业帮助

把页面动作写回业务事实，减少跨表查找、口头交接和重复确认；数据是否带来结果仍取决于流程执行与团队纪律。

客户 360 档案

把联系人、可信联系方式、公司信息、阶段、标签、交易和系统记录归入一处。



落地能力

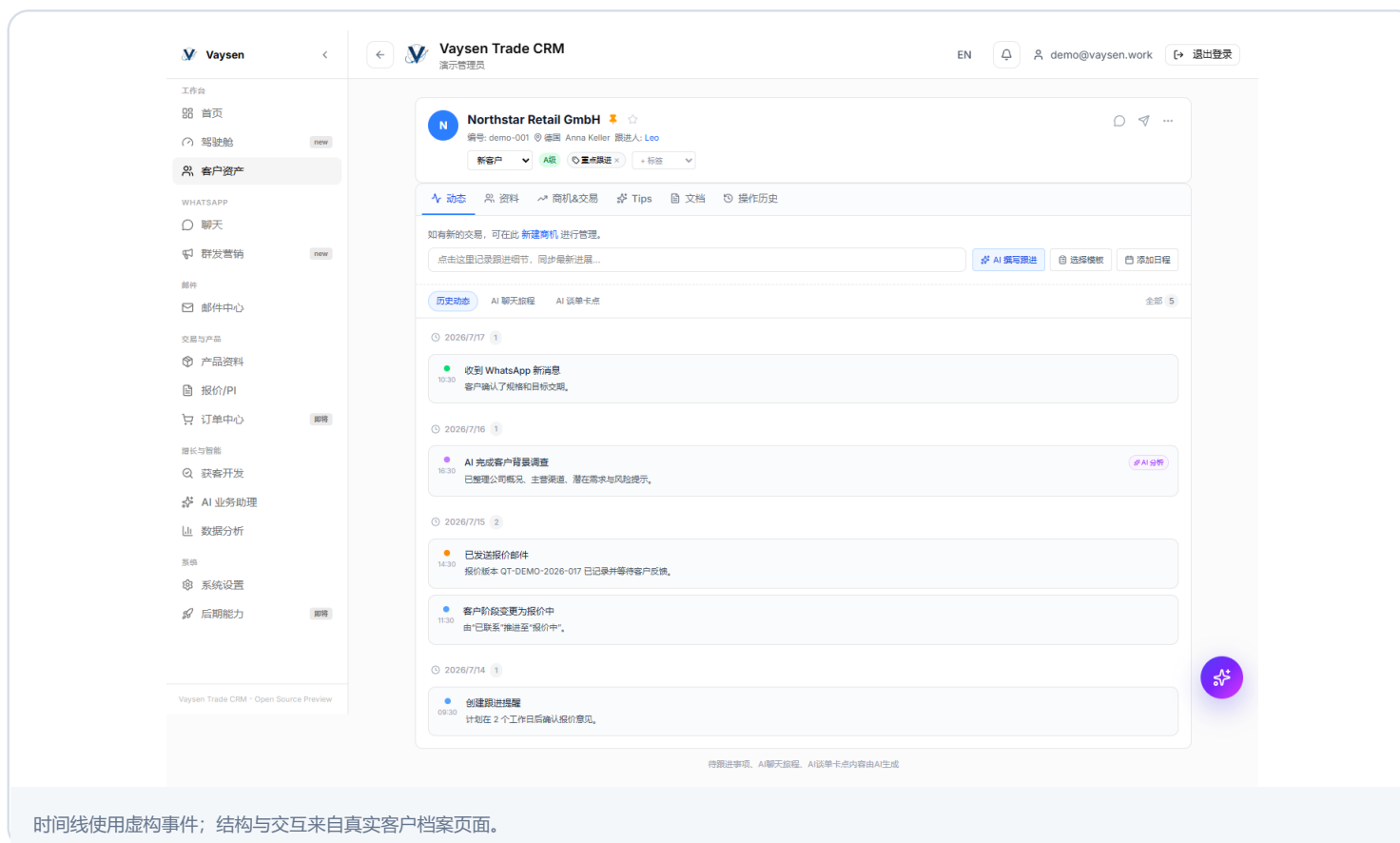
- 联系人、邮箱、电话、WhatsApp、网站、国家、来源和业务资料统一展示。
- 阶段、等级、标签、负责人和收藏状态可在档案顶部操作。
- 动态、资料、商机与交易、Tips、文档和操作历史使用同一客户主键。
- 可信身份不足时提示人工补齐，不按相似姓名或号码尾号自动合并。

企业帮助

把页面动作写回业务事实，减少跨表查找、口头交接和重复确认；数据是否带来结果仍取决于流程执行与团队纪律。

客户时间线与跟进

让所有人知道发生过什么、是谁做的、下一步是什么。



落地能力

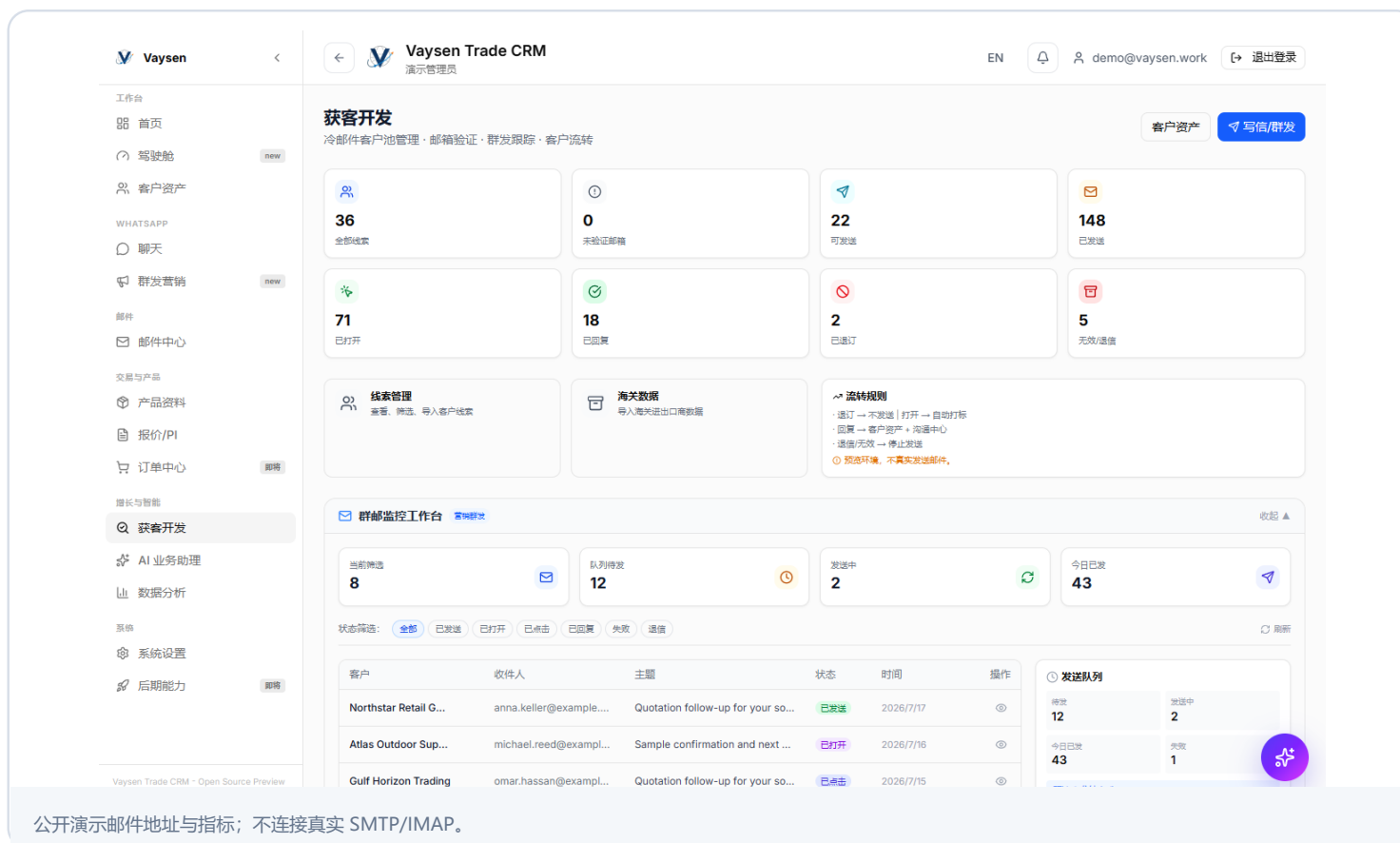
- WhatsApp、邮件、AI 背调、阶段变化、报价和提醒进入统一时间线。
- 可记录跟进细节、调用 AI 生成草稿、选择模板和安排日程。
- 按历史动态、AI 旅程和谈单卡点筛选，适合复盘与交接。
- 时间线是证据层，不应被可编辑的总结替代。

企业帮助

把页面动作写回业务事实，减少跨表查找、口头交接和重复确认；数据是否带来结果仍取决于流程执行与团队纪律。

获客开发与群邮监控

把线索池、邮件质量、发送队列、团队表现和客户流转放进同一个运营页面。



落地能力

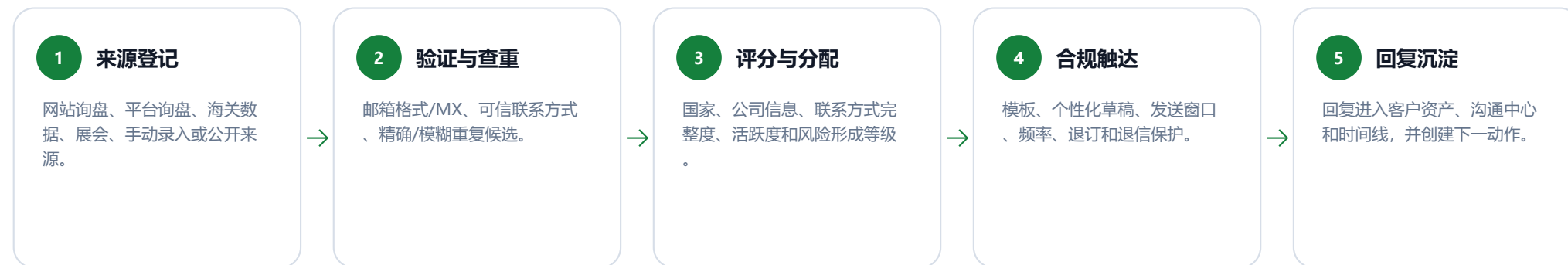
- 显示全部线索、可发送、已发送、打开、回复、退订和无效/退信。
- 群邮监控含筛选、队列待发、发送中、今日已发与失败。
- 业务员概况帮助管理员发现队列堆积、打开率异常和失败。
- 打开/点击受客户端拦截影响，只能用于趋势，不能当作确定意向。

企业帮助

把页面动作写回业务事实，减少跨表查找、口头交接和重复确认；数据是否带来结果仍取决于流程执行与团队纪律。

从线索到客户资产：一条可治理的流转链

导入、验证、查重、评分、分配、触达、回复与沉淀不再是彼此独立的动作。



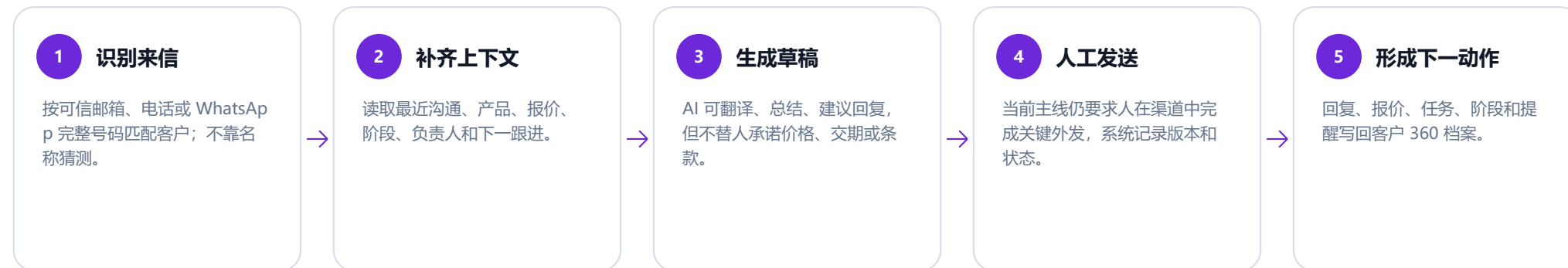
控制点	系统机制	避免的问题
数据来源	要求 source_url / 来源类型，不绕过登录、验证码和付费墙	无法解释线索从哪里来
客户身份	完整邮箱、E.164 电话/WhatsApp、显式合并	同名串客、尾号误配
发送资格	退订、黑名单、硬退信、角色邮箱与频率限制	无效触达和域名信誉损失

合规边界

开源软件不替代当地法律判断。部署者必须确认数据来源、合法利益/同意基础、隐私告知、退订、保留期限和跨境传输要求。

沟通不是独立收件箱，而是客户经营的一部分

邮件、WhatsApp、网站询盘和报价附件都需要落回同一个客户身份与时间线。



渠道	当前能力	需要额外配置
邮件	账号、模板、AI 草稿、队列、发送、打开/点击、回复、退信、退订	SMTP/IMAP、SPF、DKIM、DMARC、发送政策
WhatsApp	聊天工作区、客户关联、广播入口、报价文件准备	渠道账号、会话状态、合法联系基础
网站询盘	统一进入沟通中心并关联/创建客户	网站表单签名、限流、反垃圾

为什么暂不默认自动外发

翻译和草稿错误通常可被人发现；自动发送错误会直接触达客户并造成商业承诺。系统因此把“生成内容”和“代表企业发送”视为两个不同权限。

外贸文档中心：报价、PI、合同与样品单

把文档类型、版本、客户、金额、产品行和状态结构化。

Vaysen

工作台

首页

驾驶舱

客户资产

聊天

群发营销

邮件

邮件中心

交易与产品

产品资料

报价/PI

订单中心

增长与智能

获客开发

AI 业务助理

数据分析

系统

系统设置

后期能力

Vaysen Trade CRM

演示管理员

EN

demo@vaysen.work

退出登录

外贸文档中心

报价单 · PI · 合同 · 样品单 — 文档草稿、审批与版本管理。

全部文档

草稿

待审核

已发送

已接受

5

1

1

1

1

类型: 全部

报价单

PI

合同

样品单

状态: 全部

草稿

待审核

已批准

已发送

已接受

QT-DEMO-2026-017

Northstar Retail GmbH · \$12,800 · 3 项产品

2026/7/17

PI-DEMO-2026-011

Southern Cross Imports · \$26,400 · 2 项产品

2026/7/15

SP-DEMO-2026-006

Gulf Horizon Trading · \$680 · 1 项产品

2026/7/13

QT-DEMO-2026-018

Oak & Field Commerce · \$9,600 · 2 项产品

2026/7/11

CT-DEMO-2026-004

Maple Harbor Brands · \$31,800 · 4 项产品

2026/7/9

金额、编号和公司均为虚构演示数据；不构成真实报价。

落地能力

- 支持报价单、PI、合同和样品单的统一列表与类型筛选。
- 按草稿、待审核、已批准、已发送、已接受跟踪生命周期。
- 文档与客户、产品行、金额和创建时间关联，便于版本审计。
- AI 可准备 PDF；客户、价格、条款和最终发送仍需人工核对。

企业帮助

把页面动作写回业务事实，减少跨表查找、口头交接和重复确认；数据是否带来结果仍取决于流程执行与团队纪律。

订单中心：从成交继续跟到交付

成交不是 CRM 的终点；打样、生产、质检、出货、收款和完成仍需要同一数据链。

Vaysen

工作台

首页

驾驶舱

客户资产

WHATSAPP

聊天

群发营销

邮件

邮件中心

交易与产品

产品资料

报价/PI

订单中心

增长与智能

获客开发

AI 业务助理

数据分析

系统

系统设置

后期能力

Vaysen Trade CRM

演示管理员

EN

demo@vaysen.work

退出登录

订单中心

成交客户跟单 · 打样/生产/质检/出货/收款/售后

报价中心

全部订单

进行中

已完成

待收款

全部

已成交

打样

生产

质检

出货

收款

完成

SO-DEMO-2026-021	生产	Southern Cross Imports · \$26,400	2026/7/17
SO-DEMO-2026-019	质检	Pacific Choice Distribution · \$18,600	2026/7/14
SO-DEMO-2026-016	出货	Summit Consumer Goods · \$42,750	2026/7/11
SO-DEMO-2026-014	收款	Bluewave Sourcing · \$15,800	2026/7/8
SO-DEMO-2026-008	完成	Evergreen Wholesale · \$33,600	2026/7/5

Vaysen Trade CRM · Open Source Preview

真实订单页面；订单编号、金额和客户均为虚构演示数据。

落地能力

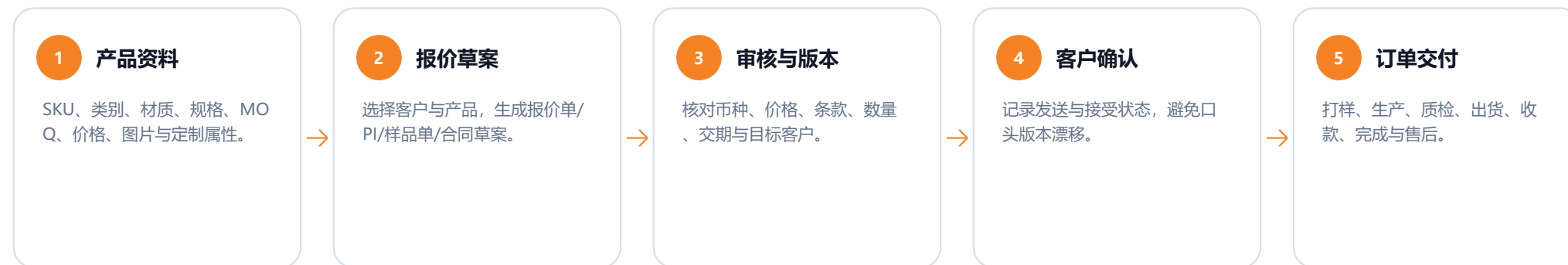
- 按全部、已成交、打样、生产、质检、出货、收款和完成筛选。
- 订单关联客户、报价金额、阶段和时间，避免成交后回到 Excel。
- 经营层可查看进行中、已完成和待收款数量。
- 当前入口仍标记“即将”，开源版应把它列为 Beta 而不是完整 ERP。

企业帮助

把页面动作写回业务事实，减少跨表查找、口头交接和重复确认；数据是否带来结果仍取决于流程执行与团队纪律。

产品、报价和订单需要共享同一份规格与版本事实

否则业务员每次报价都在重新拼表，订单阶段也无法追溯到当时承诺。



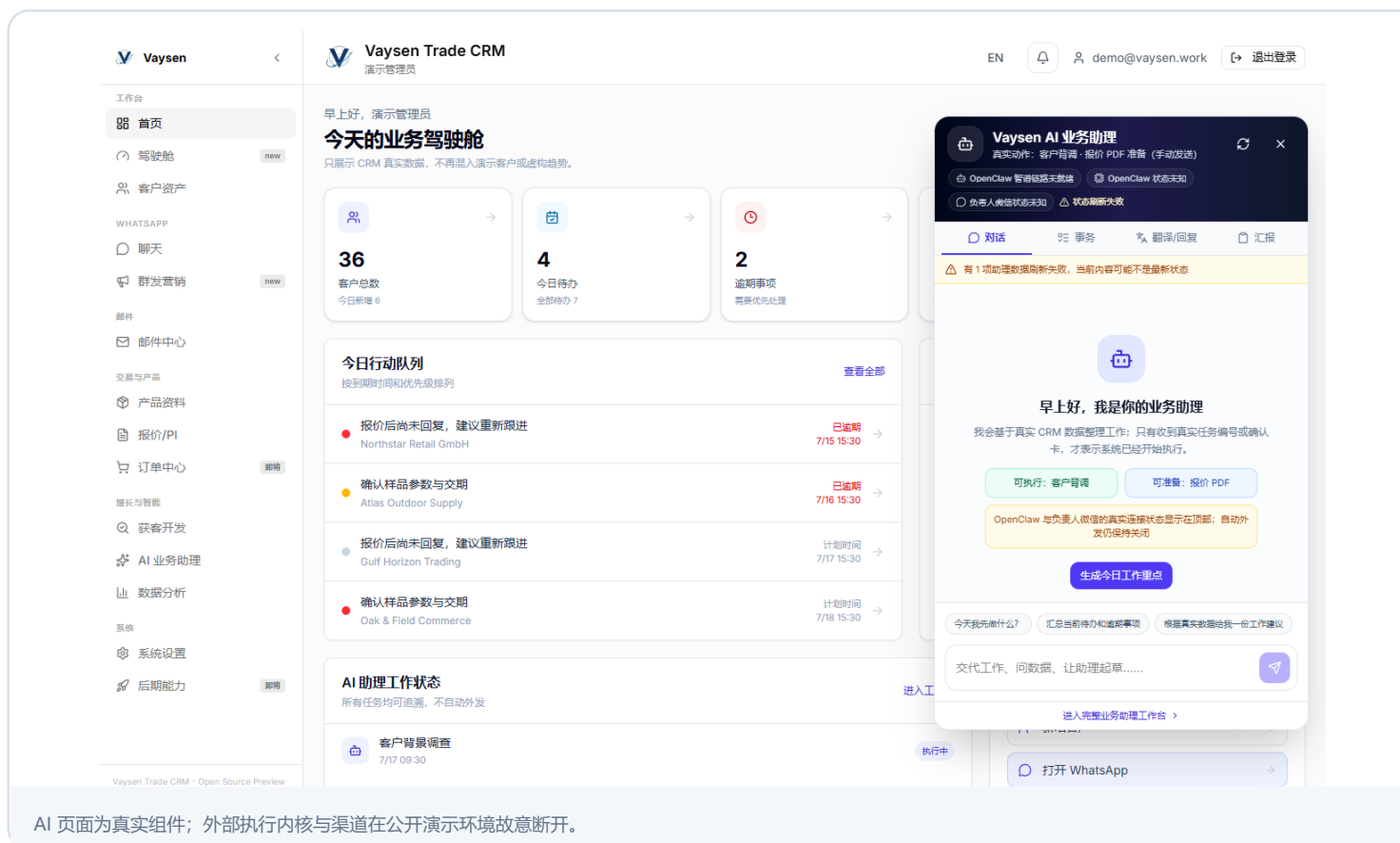
业务对象	必须保存的关键字段	系统作用
产品	SKU、规格、材质、MOQ、价格、图片、定制项	让报价基于结构化资料
报价/PI	客户、版本、币种、产品行、总额、条款、状态	让修改和审批可追溯
订单	关联报价、客户、阶段、金额、交付节点	让成交后工作继续留在同一系统

当前成熟度

报价/PI 主链已有真实页面和 PDF 准备流程；订单中心页面和阶段模型已存在，但导航仍标记“即将”，开源版应在正式承诺前补齐订单详情、权限、库存/物流边界与验收。

全局 AI 悬浮助理

在任何业务页面呼出助理，但只允许它看到当前用户和租户有权访问的数据。



落地能力

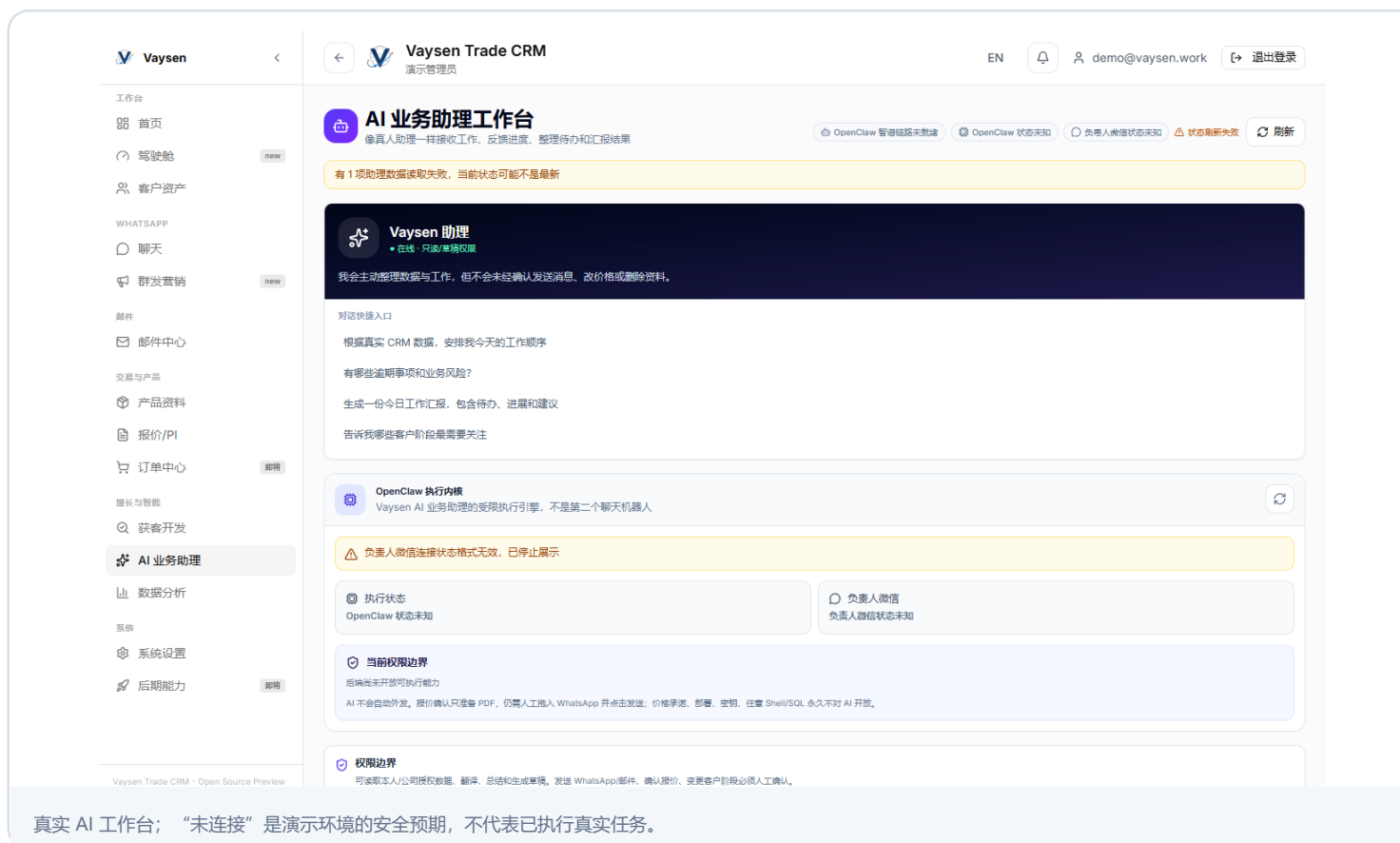
- 对话、事务、翻译/回复和汇报四类入口对应真实业务动作。
- 助理可以基于 CRM 数据组织工作，不用业务员反复复制上下文。
- 执行内核、渠道和负责人绑定状态在界面显式显示。
- 演示环境没有连接真实执行器，因此状态警告体现 fail-closed。

企业帮助

把页面动作写回业务事实，减少跨表查找、口头交接和重复确认；数据是否带来结果仍取决于流程执行与团队纪律。

AI 业务助理完整工作台

长任务、待办、工作简报、客户工具与权限边界集中管理。



落地能力

- 左侧对话区接受自然语言任务, 右侧展示简报、进行中事务和待办。
- 客户背调等长任务具有 run、状态、开始时间和可取消入口。
- 工作台明确写出自动外发、价格承诺、部署、密钥、Shell/SQL 的边界。
- 当前演示内核未连接, 页面保留警告而不伪造成功状态。

企业帮助

把页面动作写回业务事实, 减少跨表查找、口头交接和重复确认; 数据是否带来结果仍取决于流程执行与团队纪律。

AI 助理的核心不是聊天，而是受限工具、授权和回执

当前已验证主线坚持“读与准备优先，外发与高风险写入受控”。

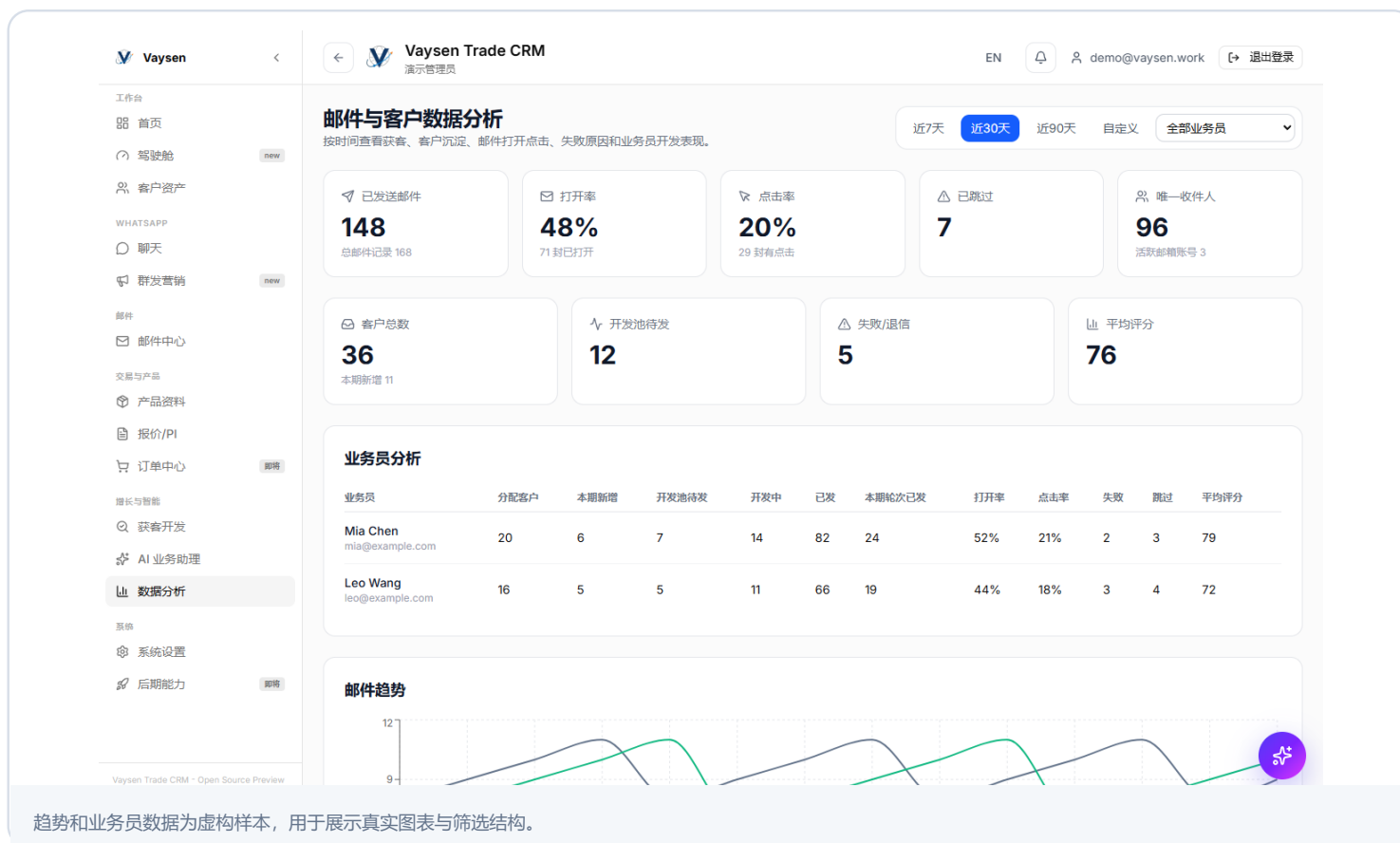
能力	当前状态	是否自动执行	人工责任
工作简报	READY	读取后直接返回	判断优先级和资源安排
客户检索	READY	只读	确认目标客户是否唯一
客户背景调查	READY	创建内部任务	核证来源与结论
准备报价 PDF	READY	生成待发送文件	核对客户、价格、条款并手动发送
自动写备注/标签/阶段/待办	BUILDING	拟通过授权执行	检查动作范围与结果
WhatsApp/邮件/微信外发	BUILDING	仅一次性或短时授权	最终确认目标与内容
删除/取消/低价/大折扣	BUILDING	强化确认	管理员承担商业责任
Shell/SQL/SSH/Docker/密钥	DISABLED	永久不向 AI 直接开放	独立运维流程

当前路线图状态

TASK-117A 权限基础已形成提交；117B-F 的客户/订单工具、真实发送、微信入口、对话 UI 与完整验收仍在开发。白皮书没有把它们写成已发布功能。

邮件与客户数据分析

把发送质量、客户沉淀、失败原因和业务员表现放在同一时间范围内观察。



落地能力

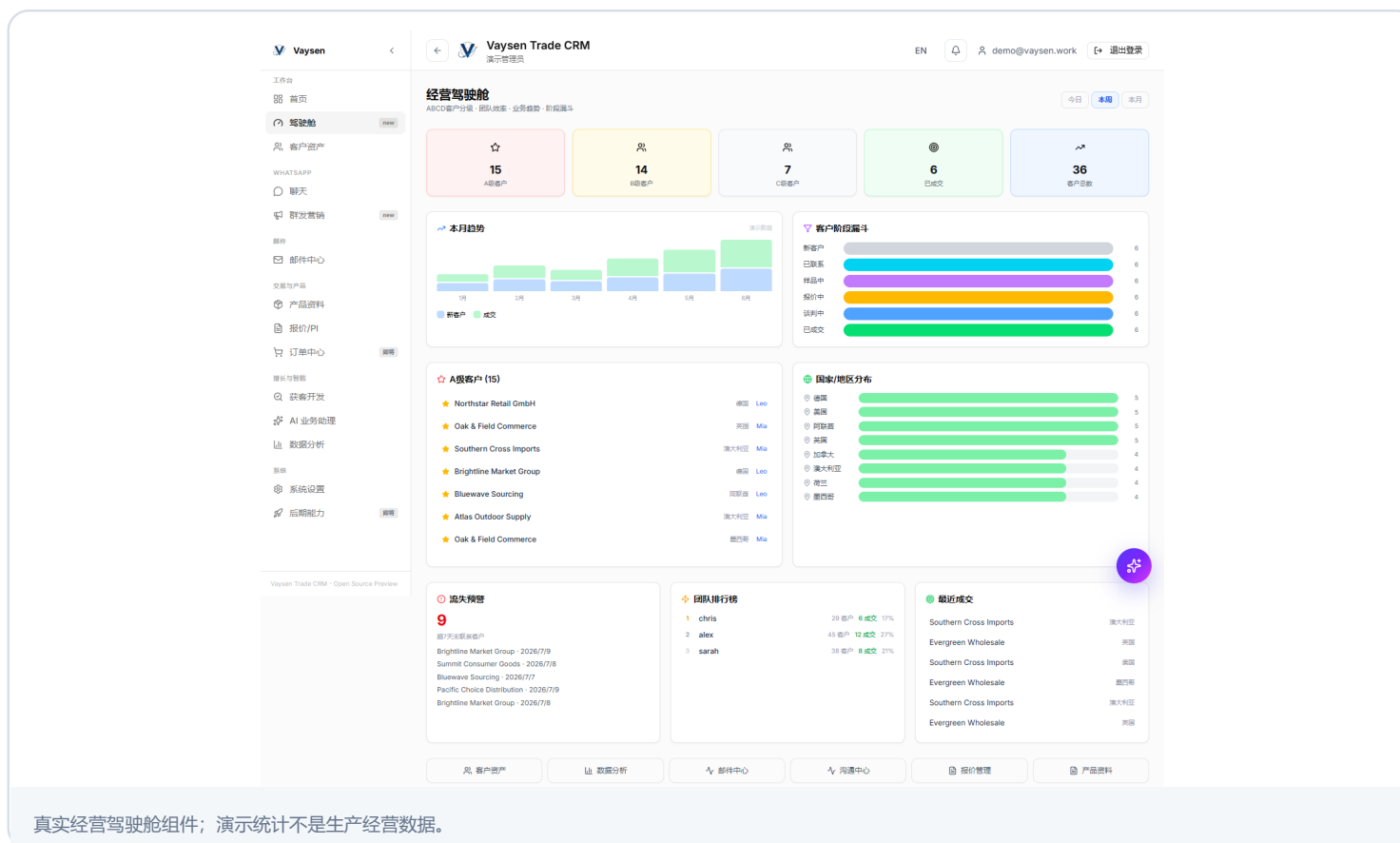
- 邮件发送、打开率、点击率、跳过、唯一收件人和活跃账号。
- 客户总数、本期新增、开发池待发、失败/退信和平均评分。
- 业务员分配、新增、待发、发送、打开、点击、失败与评分对比。
- 支持近 7/30/90 天、自定义时间和业务员筛选。

企业帮助

把页面动作写回业务事实，减少跨表查找、口头交接和重复确认；数据是否带来结果仍取决于流程执行与团队纪律。

经营驾驶舱

老板和销售经理从客户质量、漏斗、国家分布、失联和成交看业务状态。



落地能力

- A/B/C 级客户、成交与客户总量形成质量概览。
- 客户阶段漏斗、国家/地区分布和高价值客户列表。
- 失联预警、团队排行榜和最近成交帮助例会聚焦异常。
- 演示页面中部分趋势为展示性数据；开源版应全部接入真实查询。

企业帮助

把页面动作写回业务事实，减少跨表查找、口头交接和重复确认；数据是否带来结果仍取决于流程执行与团队纪律。

不同角色看到的是同一事实的不同视角

权限不是隐藏菜单，而是限制数据范围和可执行动作。

角色	主要视角	典型动作	不可越过的边界
Sales User	自己的客户、沟通、任务、报价	录入、跟进、发信、准备报价	不能管理用户、全局设置或删除他人资产
Sales Manager	团队客户、漏斗、超期与绩效	分配、检查队列、指导推进	不直接管理系统级密钥与部署
Company Admin	企业全量业务与配置	用户、角色、账号、黑名单、审批	仍不能绕过审计和数据隔离
Viewer	授权的只读数据	查看客户与结果	不能写入、发送或导出敏感数据
AI Assistant	最小授权的业务上下文	读取、总结、创建受限任务、准备文件	不拥有通用数据库、Shell、密钥或默认外发权

多租户数据隔离

请求必须带有效身份和企业上下文；管理员只能访问自己所属企业，业务员按 owner/team 范围访问。任何新模块都应在查询层继承 companyId/owner 过滤，而不是只靠前端隐藏。

能落地的企业场景

不承诺虚构 ROI；这里描述的是系统可减少的过程摩擦和可观察的改进。

业务员离职交接

客户、沟通、报价、附件、负责人和下一动作都在时间线上，新人能按事实接续。

报价后无人跟进

系统生成超期提醒，首页和负责人队列可见，避免高价值客户被聊天列表淹没。

同一客户重复开发

导入和建档先做身份锚点与重复候选，管理员显式合并，保留审计记录。

老板看不到真实过程

驾驶舱展示阶段、等级、失联、团队、邮件与成交，而非只看人工周报。

群邮损害发件域名

频率、暖机、发送窗口、退订、黑名单、硬退信和角色邮箱规则形成防线。

AI 误发或越权

工具白名单、RBAC、临时授权、幂等、回执、容器隔离与默认失败关闭。

建议测量

上线前后比较：逾期任务数、无下一动作的重点客户数、重复客户处理时长、报价版本返工、退信/失败率、客户归属争议、数据导出时间和关键动作审计覆盖率。

技术架构：Web + Windows 客户端 + 模块化后端 + 队列 + 数据层

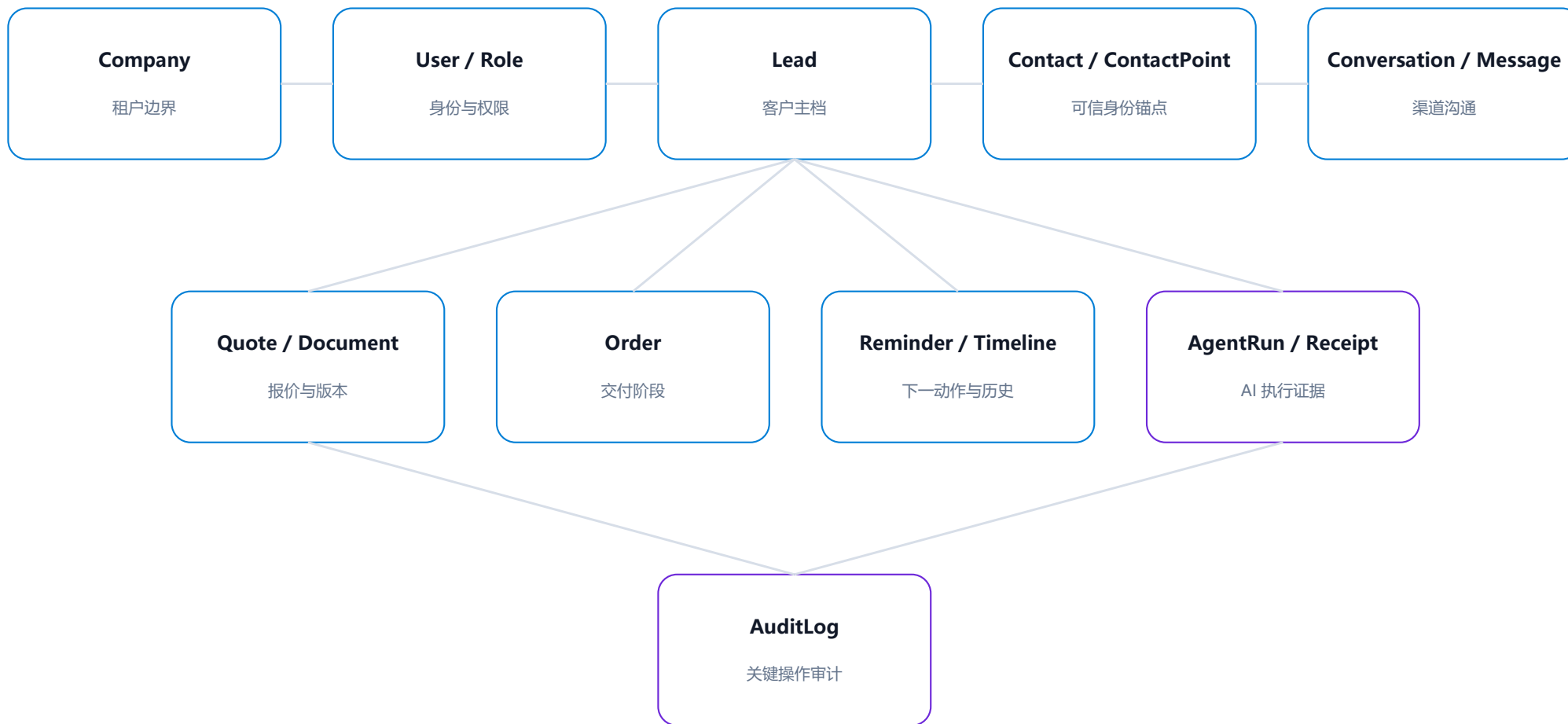
当前技术栈以可部署、可隔离、可复现和适合中小外贸团队为目标。



设计选择	原因	带来的工程收益
Web 与 Electron 双目标	办公室可用浏览器，个人电脑可装桌面端	共享业务代码，按场景分发
模块化 NestJS	客户、邮件、订单、AI 等边界清晰	便于裁剪、测试和权限复用
队列与 Worker	邮件、背调、搜索等任务耗时且需要重试	不阻塞 API，可观察进度
Docker + 固定运行时	减少 Windows/Linux 差异	发布、回滚、健康检查更可复现

核心数据模型：客户不是一个表，而是一组可追溯关系

系统用企业、用户、客户、联系方式、沟通、报价、订单、任务和审计构成业务事实图。



身份合并原则

可信联系方式优先、候选重复显式审核、合并保留旧值和审计；不因为名称相似或号码尾号相同自动把两家公司变成一个客户。

认证、密码、密钥和数据隔离

以下为代码可核验的主要机制；仍需部署方正确配置 HTTPS、密钥、备份和日志。

控制面	当前实现	说明
用户密码	bcrypt, cost 12	数据库只存哈希；登录用 bcrypt.compare 验证
访问令牌	JWT, 默认 15 分钟	短期 access token；失效后用 refresh token 换新
刷新令牌	随机 UUID 组合, 默认 7 天	数据库记录、轮换时撤销旧 token、注销可撤销
邮箱凭据	AES-256-GCM	scrypt 派生 32 字节密钥, 随机 16 字节 IV, 并保存认证标签
请求防护	Helmet、校验管道、限流	HTTP 安全头、DTO 校验、API/业务频率限制
授权	RBAC + companyId/owner 数据过滤	角色与数据范围共同决定能否访问
数据库	Prisma 参数化查询	降低 SQL 注入风险；仍需最小数据库权限
审计	AuditLog、Timeline、Agent Receipt	关键操作、业务变化与 AI 动作留下证据

必须改进的开源默认值

当前加密工具允许缺省 salt 常量，仅在未提供环境变量时使用。开源发布应要求每个部署生成独立 salt/key、加入密钥轮换说明，并增加泄漏扫描与启动时强校验。

AI 执行安全：让 Agent 只能做被定义过的业务动作

OpenClaw 与 CRM 之间不是“给一个管理员 Token”，而是一个受限制的 broker。



隔离措施	实现方向	被阻止的风险
只读根文件系统 / cap_drop ALL	容器最小权限、no-new-privileges、PID 限制	Agent 借容器权限控制主机
不挂载数据库/Redis/SSH/Docker socket	只访问专用 backend 接口	越过业务权限直接改数据或部署
固定工具白名单	工作简报、检索、背调、报价准备等明确能力	提示词诱导调用任意系统命令
失败关闭	状态未知、目标不唯一、授权过期即拒绝	网络或状态异常时“猜着执行”

不能混淆

模型推理安全、工具权限安全、渠道账号安全和企业业务审批是四层不同问题；任何一层缺失，都不能靠“提示词写得更严”替代。

邮件与客户数据治理

系统提供合规机制，但是否满足具体国家/地区法律仍由部署者评估。

退订

唯一不可猜 token、一键退订、立即取消待发送、标记 Do Not Contact。

黑名单

系统/企业/客户三级规则，硬退信、投诉与人工屏蔽进入发送前检查。

频率与暖机

账号日/小时上限、最小间隔、客户间隔、Campaign 上限和渐进暖机。

发送窗口

可按客户当地时间限制触达，减少非工作时段打扰。

退信治理

硬退信立即停发；软退信按策略重试；异常退信率暂停账号。

数据权利

支持导出、删除、保留策略和审计；敏感信息不应被采集。

部署者责任

不要购买、抓取或导入来源不明的数据；不要绕过登录、验证码、付费墙或平台条款；不要把打开像素当成确定事实；应按适用法律配置隐私告知、合法基础、退订、保留、访问和删除流程。

部署形态与运维边界

系统支持局域网/私网后端与 Windows 客户端，也可以按开源用户自己的基础设施改造。



部署项	当前状态	开源用户注意
Linux Docker 部署	已有 compose、脚本、健康检查、备份/回滚合同	先在新环境恢复演练，再连接真实数据
Windows 安装包	已有 Electron 发布链，当前安装包未代码签名	用户会看到未知发布者提示；正式分发应签名
更新	当前以受控手动分发为主	不要在签名/回滚未闭环前启用自动更新
公网访问	不建议直接暴露后端	使用 HTTPS、WAF/反向代理、私网或零信任接入

最小生产要求

独立密钥、HTTPS、最小端口、数据库私网、非 root 容器、备份校验、恢复演练、日志限额、监控告警、管理员 MFA（当前需补充）、代码签名与漏洞更新流程。

工程证据：功能介绍之外，还要证明系统能被重复构建和恢复

下面是 2026-07-16/17 内部发布资料中的验证快照，不等于第三方认证。

v1.4.20

当前发布线

16

运行容器

6/6

Worker 健康

27/27

独立 LAN Smoke

374

Electron Jest

11/11

统一门禁

验证类别	覆盖内容	为什么重要
构建与类型	前端 Web/Electron、后端、Prisma、Node 20 门禁	避免 “只在开发者电脑能跑”
数据库	迁移、fresh DB、备份、恢复、回滚与数据指纹	升级失败时能回到一致状态
安全	HMAC/nonce、租户/RBAC、幂等、敏感信息脱敏	防止 Agent 或接口越权
浏览器	多视口、双标签、断网重试、AI 悬浮层	验证真实交互和并发边界
运行时	容器、Worker、健康检查、零重启、日志与镜像版本	证明发布后的系统仍健康

公开后需要重跑

开源仓库、依赖、品牌脱敏、示例配置和安装路径发生变化后，以上数字必须新的公开基线重新生成，不能直接沿用客户定制版证据。

现在是“准备开源”，还不是完整开源发布

README 写有 MIT 意图，但仓库根目录没有正式 LICENSE 文件。没有 License，外部用户没有明确的复制、修改和分发授权。

发布项	当前状态	开源前动作
LICENSE	缺失；README 仅写 MIT License	添加正式 MIT LICENSE，确认所有代码版权归属与可授权范围
客户品牌与数据	代码和文档仍有客户定制痕迹	全仓扫描名称、域名、邮箱、账号、logo、路径、测试样本和截图
密钥与历史	当前工作区不能视为可直接公开	扫描 Git 历史、release、日志、env、备份、安装包和 issue 附件
第三方 License	依赖多，含渠道、浏览器、AI 与媒体组件	生成 SBOM/NOTICE，核对直接与传递依赖 License
示例配置	生产配置和私网路径不可公开	提供 .env.example、demo seed、最小 compose 与安全默认值
品牌命名	需从客户专属品牌迁移为公开产品名	完成 Vaysen Trade CRM 品牌替换，不破坏客户部署升级
贡献治理	尚未形成公开协作文件	补充 CONTRIBUTING、SECURITY、CODE_OF_CONDUCT、issue/PR 模板

最重要的一句

把私有仓库切成 Public 不是开源流程的最后一步，而是数据泄漏风险最高的一步。必须先在全新公开仓库导出干净快照，并由人工复核历史。

企业落地建议：先跑一条真实闭环，再扩展

不要一上来导入全部历史数据、接通所有渠道并开启自动化。



上线前	上线中	上线后
确认数据合法来源	每日检查异常与逾期	每周复盘阶段变化和失联
配置角色和最小权限	抽检客户身份与报价对象	按月恢复演练与依赖更新
建立字段字典和阶段定义	记录未进入系统的旁路工作	清理无 owner、无下一动作数据
备份数据、设置数据血缘	保持 AI 外发前记录可追溯	根据汇报逐步接入自动化

成功标准

不是“导入了多少客户”或“AI 回答了多少次”，而是团队是否用同一事实工作、关键客户是否有下一动作、重要变更是否可追溯、系统故障是否可恢复。

模块清单（按业务域归类）

代码树包含 38 个后端模块目录和 70 个 page.tsx；以下是公开介绍中最相关的业务域。

业务域	后端/前端能力
客户与组织	auth, companies, users, leads, tags, customer-identity, duplicate-leads, timeline
获客与研究	search, continuous-prospect, deep-research, imports, external-leads, lead-scores
邮件	emails, email-accounts, email-templates, email-track, email-events-sync, business-mail, mail-workbench
沟通	communications, whatsapp, customer-workspace, inbound inquiry, conversation/message UI
交易	products, materials, customizer, quotes, orders
任务与管理	follow-up-reminders, queues, dashboard, analytics, executive, system-admin
AI 与自动化	ai, agent, ai-communications, openclaw, assistant runtime, workbench, receipts
暂未公开主线	voice-customer-service / voice-service（发布开关隐藏）

统计注意

页面和模块数量是工程结构，不是功能价值排名。开源版应以“能否完成真实闭环、是否有测试、是否有权限边界、是否可部署恢复”作为成熟度标准。



把客户、沟通、报价、订单和 AI 放进同一条可追溯工作链。

Vaysen Trade CRM 的开源目标，不是复制某家企业的定制系统，而是沉淀一套外贸团队可以自托管、扩展和审计的业务基础设施。

联系与项目入口

网站: vaysen.work 邮箱: info@vaysen.work 微信: vaysenai