

分析师 1:

大家好，欢迎参加华源传媒互联网团队 AI 应用新“栋”察（十七），AI 竞争进入 Huns 时代，目前所有参会者均处于静音状态，下面开始播报声明。

分析师 2:

各位投资者下午好，我是华源传媒魏征。那我们发现，现在整个 AI 产业发生了一个比较重要的一个变化，就是当下的一个 AI 的竞争重点正在从大模型能力逐步的转向 Harness 层，也就是智能体运行时系统和工程化交付能力这一块。那过去大家其实更关注的是模型参数，benchmark，然后 token 的价格呀，包括一些性能的评测排名等等。那其实我们现在发现下来，就是 AI 还是要运用在各个场景的，包括 coding 场景，然后现在讲的 work 场景。

那所以说很多一些各种场景的里面的一些企业它真正愿意去付费的其实并不是模型本身，而是模型能不能去接入你的业务系统，能不能去和你的本身的行业的一些场景去进行融合，来实现一些场景内的一些价值。那其中，一些核心能力，比如说，这个主要就是关乎于 Harness 层了。那在模型之外，你这个模型能不能去调用你企业的数据，调用你企业内部的一些工具，能不能按照你的企业的自身的一些工作流，在权限之内，在安全性之内去完成一些任务，并且能够持续的稳定的去产生结果。

那其实这个是很多场景，包括一些企业呀，政府端，他们所关心的一些问题。那我们先从一个简单的问题开始，那到底 Honeys 是什么？那很多人其实还没搞懂这个问题。那我们其实可以把 AI Agent 去拆解成一个简单的公式，就是 AI Agent 等于大模型加 Honeys。大模型它负责思考，然后负责推理，相当于一匹野马或者说一辆车，但有时候它就很容易放飞自我，这个时候我们就要为这匹马，为这个模型去装上一些工具，比如说 skill 权限，然后记忆系统，然后包括怎么去执行，一些脚本等等，相当于马鞭、马鞍一整套的这种驾驭的工具，这样就能够驯服这匹野马，让它能够在真实的场景中，在公司的业务系统中不会跑偏，而是根据一个正确的方向，正确的工作流去进行一个任务的执行，最终重复给你一个正确的结果。

所以说简单来说，Honeys 就是帮你去。驾驭 AI 大模型的一个一整套的系统。那为什么 Harness 最近特别火？因为大家发现，在同样的大模型装上不同的 Harness 之后，Agent 它的一个执行能力会有很大的差距。比如说我们看 OpenAI 的官网披露的这个例子，那在 ARCAGI 三测试中，OpenAI 发现，在 Harness 层面中，开启一个保留推理和上下文压缩的这样一个功能之后，Harness 的机制能够显著的去改善它那个 Agent 的长期任务执行能力。

那 GPT-4.5 So1 的得分从 13.3 提升到了 38.3，同时它的输出 token 减少了六倍。所以说这个结果表明了什么？那第一点，Harness 它会直接影响你基模，影响你模型的表现。那同一个模型在不同的记忆、上下文和工具的调用机制之下，可能会得到完全不同的结果。那第二点，Harness 能够显著的改善产生的效果以及。你的 token 的成本。实际上，Agent 的能力不是模型能力的简单叠加，它实际的效果。尤其是在具体的场景中，取决于模型，也取决于你的上下文管理，你的工具调用，你的权限控制，包括各种的 Harness 中的一些组件的共同的一个作用。

然后，前段时间，DeepSeek 它是开源了它那个 Connis 桌面版的一个应用。那安装方式，

就是我们直接通过这个网站就可以下载，打开就是这个样子，就其实也很类似于 Work Buddy CodeX 这种桌面端的应用助手的。那它们的。差别在于什么？那我们可以看一下，那我们在进入 DeepSeek Harness 的这个界面之后，我们先选择一个本地文件夹，来选择一个项目或者说你的工作空间，那后续我们所有的操作都是在这个文件夹里面。然后，这边我们可以修改操作权限，包括三种的权限等级，分别是只允许读取，可以修改写入，然后还有完全访问。

然后，这边还可以切换模型，包括推理等级的高低。然后，我们还可以直接在设置里面，自定义去添加各种各样的模型。那这就是和其他的一个 agent 的一个区别，就是 DBCA Harness 这边的模型你可以自定义，那你像其他的，我和巴迪，和戴尔萨，他们都是已经帮你预设好的一些模型。那这边就是自定义的程度会更高，那里面所有的那种小的功能我们都可以自由的开启，然后卸载。然后在这边的选项里面，我们可以看到有几种模式可以选择。那这个功能是什么？

就是说我们可以去预设一个绘画的 agent 中运行的一些插件组装，比如说我们在。某一个场景里面，它的工具、提示词和能力，我们可以去自由的去组装、去自定义。那前三种，标准模式、PTC 模式、极简模式是它帮你预设好的，最后一个创造模式，那我们可以根据不同的场景去进行一些预设。那首先我们一个讲，第一个是标准模式，那它就是一个功能完整的一个编码 agent，那支持文件的编辑，包括文件和网页的搜索，skill，目标，子代理，然后工作流等等，它是一个比较完整的一个模式。

第二个是 PTC 模式，它除了具有标准模式的全部能力之外，还通过 code mode SDK 去呈现一些工具，让模型可以用一个 TypeScript 程序去组合多步的操作，也就是说能够去进行批量的处理，批量的工作流，这是 PTC 模式。第三个是极简模式，它就是只提供一个持久的 bash 和一些编程，它主要是适用于一些。这个，测评的场景，主要是给开开发者去进行一个测评的一个模式场景。最后，是一个创造模式，那我们不同的开发者，不同的用户可以基于自己的工作流去进行自定义，可以去进行自定义。

那就在上周，CodeX 也是开源了它的 Harness，但是，它和 DeepSeek 的 Harness 的开放程度和它们的侧重点，实际上是不一样的。那 DeepSeek Harness 刚才我们通过这样一个展示能够看到，它更加强调在 AI Agent 的运行时本身的一些工具、模块，它的一个可替换性，你可以随意的启用、关闭、卸载、替换。那 CodeX Harness 和这个也不一样，它并没有去开放它那个 CodeX Harness 层的一些工具，它而是说更加去强调将 CodeX 本身的一个 Agent 的能力。

它开放给第三方，作为一个 MCP，能够让你的第三方在具体的场景中，将 Codex 的 Harness 嵌入进去，实现一个业务系统层面的一个结合，那他们是这两个侧重点。我们再具体比较一下，那从开放性的角度来说，我们直接看到 DeepSeek 的 Holistic 官网，它有个 slogan 叫一切皆插件，就是说，DeepSeek 它的一个理念就是将工具、模型、skill、绘画、刷箱、一定的循环调度、UI 等等，全部作为可以。一个插件进行一个替换或者重新组合，它那它的一个开放性，更加偏向于一个底层，底层的一个系统。

那 Codex 这边，它的开放重点是在于 Harness 层与和应用层之间的一个集合层，那它是，我们看到这个图，Codex 它是提供了 Codex CLI、SDK 然后 App Server 三个小的这样一个工具。那它的作用是什么？就是你的开发者能够通过这几样插件让 Codex 这个 Agent 嵌入

到已有的系统和产品中，这个就是我们说的，很多企业，公司，政府系统，会招这种 FD 一，招招几个 IT 进来去去把 AI 和你本身的一个企业系统去进行融合，那 Codex 就是开放了这个能力，让你的开发者能够将自己的业务系统。

自己的知识库。打通到 Codex 里面去，那但是，Codex 它底层的一些工具，都是非开源的，就是你调用不到的，它只是开放了和应用层之间的这一个集合层，这幅图就是 Codex 官网展示的，一个物流的系统 and Codex 它们打通去进行结合。那我们可以看到这里面，Codex 的应用层就不再是我们平时用的这种通用性的助手了，而是完全的嵌入到你的业务系统中，Codex 能够读取到你的，公司内部系统中的订单呀，运输状态呀，一些业务数据等等，然后它能够通过自身的一些能力，去进行一些信息的获取，一些分析，然后最终给出建议。

那对于 Harnes 在一个具体的场景去落地的一个很重要的一个项目就是腾讯的 WorkBody 前两天它是做了一个这样一个私有化的部署。那这个项目是由数字广东、广东省政务局等主体去和腾讯的 Work Body 去合作推进的。那腾讯主要去负责 Work Body 私有化部署的相关内容，那整个这个项目的金额就是按项目制收费，大概就 3000 多万，3000 多万元，不包含服务器和算力采购的费用。然后整个这个项目中的合同内容主要是包括 Work Body 私有化部署，然后去定制化你的 workflow 开发 skill，线上交付以及最后是三年运维的服务。

那首批试点这个项目首批试点包括在广东，广东的那个数字广东，广东省广东省政数局、省医保局，然后中小企业服务中心，一共覆盖大概 800 个席，8000 个席位，8000 个席位。目前是上线了一百多个 skill，然后搭建了三到四亿条的一个公共政策知识库。所以说，从 Work Buddy Finance 这一层的具体落地来看，它主要是完成了四类工作。第一个，搭建了政务务的知识体系，知识库。那它把全省的公共政策知识，然后包括各部门专属的知识库全部接入到了这个叫做秦湾的智能体这个 Work Buddy 里面。

第二个就是构建一个 workflow 和 skill，那针对具体具体的业务场景去定制化的一个开发一个 skill。那第三个就是完成了国产化环境的适配，包括国产的芯片、服务器、大模型，全都是国产的。那第四个就是在政务系统内网，也就是业务系统里面去完成了私有化部署，那实现了数据的隔离、权限的管理，然后安全的审计。因为我们本身 C 端用的 Wokabali 都是云的，包括你的模型也都是跑在云端的，那这边这个私有化部署全部都是在本地，全部都是本地。

那从部署的方式来看，这个项目，包括我们认为，未来的这种，Harnes 层的一个企业端的对接和部署，主要有几种商业模式吧。那第一个就是面向中小型事业单位的一个公有云 SaaS 模式，那就是比如说 Work Buddy 企业版，或者说豆包办公企业版，他们是按照席位制收费的，每个席位每个月大概就是几百块钱，一年就是几千块钱。那第二类就是面向国企、城投、市级政府，然后事业单位的一个专有云模式。那包括它提供的一些服务，包括独立的 VPC 来提供隔离环境，这个也是按照席位制收费的，那这个就可能每个月三百四百元。

第三一类就是面向省级的政务项目的一个纯私有化的定制模式，那客户他自己去负责采购算力，采购服务器，那平台方只负责去进行私有化的部署、适配、skill 开发、现场交付以及后续的一些运维，那这种就主要就是按照项目制收费，那前面两种那种公有云的 SaaS 主要就是按照席位制收费，这个就跟 C 端差不多，那 C 端也是一个人每个月多少钱，你可能用的比较多，你再按照超出的那个 token 去计费，那私有化部署就是直接按



制去进行收费，一个项目可能就几百几千万。

然后从收入的结构上来说，根据我们的调研情况。整体上，C 端，这种 Workbody 这种产品，那以 Workbody 为例，C 端可能占 7%到 8%的一个收入，然后剩下 90%以上是 B 端，然后 B 端里面可以拆分成公有云、SaaS，然后私有化部署，那公有云、SaaS 这块就占比 70%左右，剩下的 20%到三十可能就是这种私有化部署。所以说从整体，这种 work agent 的市场规模来看，一定是比 call 顶的场景，它的一个，市场规模是更大的。那 call 点场景它覆盖的人群相对还是比较有限，那 agent 的场景，首先，覆盖了广泛的白领人群，包括政务，企业，一些私企，国企，等等。

第二点就是我们发现，就是。除了模线长之外，整个 Harness 产业现在也是越来越受重视的，也就是说。在落地于更加真实的一个场景之中，一定是懂行业 know how，懂 workflow、懂企业系统的，去将这个 AI 融入到你的这个部署到私有化部署到你的企业内部中去。那这个，也需要专门的公司、专门的专业的人才去进行一个处理。所以说我们认为，AI 一定是能够去重塑各种垂类行业的一个服务链路和价值分配的。那我们传统的这种 SaaS 软件，之前主要是通过一些标准化的产品，然后人工的一些操作界面去提高效率。

那现在我们进入 AI 时代，那 AI 它影响的不止只是一个软件的一个形态，而是延伸到获客、咨询、方案设计、交付、运营，然后持续优化，然后运维等等一个完整的一个服务链路。所以说，对于这种原生的 AI 及产品来说，它的一个长期价值，不仅只是一个这样一个桌面的工具，而是更多的集中在你的行业数据是不是能够接入到你的企业内部系统中去，怎么样去接入，然后也需要懂行业内耗的一个人才，懂客户关系，的这样一个公司去做这个事儿。

所以说，我们落到投资观点上来看，我们认为，未来一定是在各种的垂类的场景中，具备行业理解，具备客户触达，然后具备服务能力的这些平台，或者说传统的 SaaS 软件厂商。它能够转向 AI 的一些专业的这种机构，都有机会升级成 FD 丁一丁黄石万泉于炳麟付永翀何帅辰何理冯佳文冯逸华刘俊。