AI Agents Will Be The Key To Achieving ROI From AI

The hottest trend in the fall of 2024 will not be Pumpkin Spice Lattes (despite their deliciousness), it will be AI agents. And that heat may be justified. Why? Well, a lot has changed since early in 2024, when investors were clamoring to put high valuations on any company with AI technology. Now, as if overnight, Wall Street and others are asking for specifics about ROI. While this very rapid turn of events may be unfair, I do think agents will be key for deriving a good return from the investments fueling next-generation AI solutions and investments. Many companies such as Google and Salesforce have announced new capabilities for creating agents for business users. These task-based agents demonstrate practical uses for AI in a way that enterprises can understand, use and measure. It's a topic worth digging into.

What Is An AI Agent?

An agent is a *composite* and *autonomous* application that enables humans and AI to *collaborate* to complete a task. The italicized terms in this definition need clarification because AI-based agents are a new approach to applications. Before we get into that, it's also important to distinguish agents from existing AI-assisted copilots or chatbots, which aren't as sophisticated. For instance, the common AI chatbot interface is focused on taking a specific user command and getting a response from the LLM. An AI agent will be able to take further actions based upon the results of the LLM response, with or without further human involvement.

A composite application is one that comprises multiple reasoning or action capabilities. While the notion of composite applications has

AI Agents Will Be The Key To Achieving ROI From AI

been around for a while, in the AI space the difference they make is more pronounced. For example, an AI agent will have both programmatic or deterministic qualities as well as holistic or unstructured qualities (such as LLM prompts and outputs). It might, for example, initiate a credit check when a user asks questions about a loan; in that case, the LLM would craft a loan proposal based upon the credit score and the natural language inputs of the user, taking into account what terms other banks are offering. By contrast, trying to do the same thing using a chatbot would require multiple requests, and the user might or might not understand how to craft the prompts to get the answer they need.

AI agents will be delegated much higher degrees of freedom—autonomy—than previous applications. For example, in a business process where 80% of customer-facing transactions are easily completed, the AI agent may just handle these simpler requests from end to end and push only the 20% of exceptions to a human.

And that is where the collaboration comes into play. It would be easy to assume that an agent is some sort of slippery slope to job replacement. That's not true because of the limits of AI's current capabilities, coupled with the high number of undigitized tasks in the world that require humans to be in the loop somehow. I would even argue that "collaboration" may be too loose a term for today's AI agents, which are commonly pointed at an existing workflow. A more apt way to describe an agent today is that humans delegate work to AI agents by setting the rules, constraints, workflows and success criteria; the agent merely executes.

AI Agents Will Be The Key To Achieving ROI From AI

Why Agents Matter — The Business Explanation

An agent can be a powerful tool in the hands of a business user. By automating repetitive workflows such as gathering data and preparing reports, AI agents can give users more time to focus on more important, higher-level tasks that can't be automated. While the makers of the AI copilots and chatbots that have been introduced over the past two years have suggested this as a value proposition, proper AI agents provide substantially more benefits, including these:

1. **Agents are purposeful —** Copilots and chatbots are freeform, in that the user can ask anything it can think of to the LLM. even if it is beyond the capabilities of the LLM and no action can be taken. By contrast, an agent can be given a specific workflow or set of tools it can use to complete an activity. This level of process specificity is measurable against existing or aspirational business KPIs.

2. **Agents can be created and managed by non-developers —** Using no-code or low-code tooling along with basic prompts, agents can be developed rather easily for internal uses. In fact, Salesforce's new Agentforce platform has a number of examples where a non-technical business user can build their own agents. (I'll have more specifics about Agentforce in my next article.)

3. **Agents provide AI with better working context —** There are a number of concerns about AI solutions providing overly general—or outright bogus—answers. But by predefining the LLM prompts within the logic of the

AI Agents Will Be The Key To Achieving ROI From AI

agent and leveraging well-defined services and data, an agent can deliver more precise and contextual responses than public AI chatbots.

Let's think through an example. This year, many marketing teams used Microsoft Copilot or Google Gemini to help them select locations for company events. An agent could go further by automating a substantial part of the process of event planning. This would include considering surveys from past events, comparing site options, understanding availability of the sites and key speakers, determining travel considerations and modeling the number of sessions a particular site can host. After figuring all of this out, the agent could show you the event plan and proposed budget, and possibly even generate appropriate purchase orders or internal approval tickets. For the event planner, this will save a lot of time while still giving appropriate consideration to company preferences and controls.

Why Agents Matter — The Technical Explanation

As I learned and discussed in this recent article, there are limits to what an AI chatbot approach can do. However, as explained above, agents are different in that they are able to use both deterministic and non-deterministic methods to provide consumers and businesses with a more precise level of automation. Thinking more about the corporate event-planning scenario above, AI agents provide some very clear benefits over other types of applications.

The first benefit is integration. When it's planning the event, the agent will determine that your company prefers to fly Delta because of an existing agreement in a contracts database. By summarizing

AI Agents Will Be The Key To Achieving ROI From AI

last year's event surveys, it will know that most of your attendees prefer starting earlier in the day. And it will estimate that you can hold about 200 total sessions based upon the number of meeting rooms at the sites it's recommending.

Second is persistence. The agent can remember preferences over time. When planning future events, it will eliminate choices based upon earlier feedback, for example by avoiding a certain hotel chain or ensuring that the event has vegan-friendly food options.

Third is managing ambiguity. The natural language interface that taps into an LLM provides a better way to move forward when a process gets stuck. In deterministic applications, when in doubt, the app errors out and you get nothing. With an AI agent, it can instead ask you how to handle the situation. For instance, maybe a target date for your corporate event does not align with site availability; instead of just stopping the process, the agent can ask the user if there are any parameters that can be changed. Additionally, if something is a consistent blocker to the process, it's a simple matter of providing new options or services to the LLM rather than a major re-coding effort.

The number of rules and processes that can be mitigated by agent development versus deterministic programming will save a great deal of development time and allow companies to reach the market faster.

What Are The Components Of An AI Agent?

As you can guess, an AI agent is a fairly complex application. There are a number of great resources out there to explain what's in an

AI Agents Will Be The Key To Achieving ROI From AI

agent. I particularly like this one from IBM and this one from AWS. But here is a very high-level view and definition of the common components.

- **LLM —** The LLM serves many roles in the agent; it can guide the process or make reasoned decisions based upon the inputs it receives from the user or other applications. I also think that over time you will see agents that leverage multiple LLMs or machine learning models to achieve the specific goals of the agent.
- **Data —** This is either the application data for the programmatic elements of the agent or the inference data from the LLM.
- **Governance —** These are business rules and parameters that constrain the agent. These can include policies, guardrails or security credentials.
- **Integrations —** These are the elements of connectivity and data provenance among different applications and services.
- **Workflows / Rules —** These are what primarily guide the agent and the LLM through the process. Collectively, these are the framework for what the agent executes.
- **Human Interface —** This is where the agent and humans collaborate. This can be a dashboard or it could be something as simple as a notification on your device.
- **Persistence —** This is the memory of the agent. This is where data of interest to the agent is stored to either inject knowledge into the agent or help shape inferences.

AI Agents Will Be The Key To Achieving ROI From AI

How Does The First Year Of Agents Play Out?

As we head towards 2025, we are already seeing a great deal of excitement and lots of vendor announcements about AI agents. I believe that, like most things AI-related, agents will mature quickly. This is partially due to companies' desire to see a meaningful ROI case for AI, but it's also because of how agents will be rolled out.

I see this happening in four phases:

1. **Today: Application Platforms —** Application platforms such as Salesforce, ServiceNow or SAP will be the first movers in the agent space. Because these platforms automate business processes, agents will offer a new way for users to increase productivity. It also helps that these platforms have most of the necessary components in place, and those components are already optimized. This means that AI agents are a natural extension of a platform's ecosystem, data structures, tooling capabilities and existing AI functions.
2. **Early 2025: Infrastructure Platforms —** Infrastructure platforms including AWS and Oracle Cloud Infrastructure have many of the components as well, but these platforms are positioned for the developer and architect audience. These offerings will need to be more technology-agnostic and support more enterprise-level tools and management backbones.
3. **Early to mid-2025: Startup Pivots —** There are a lot of AI startups out there that will need to retool their strategies, if they haven't already. Loosening of monetary policy and a clear path to ROI will prompt VCs and other startup

AI Agents Will Be The Key To Achieving ROI From AI

investors to follow the money and retool their portfolio companies toward more investor value. I also see two other opportunities here. First will be the emergence of new business models such as event-planning agents that charge a flat fee per plan. There is also the very real possibility of an agent "store" or marketplace sponsored by a Phase 1 or Phase 2 leader.

4. **Mid- to late 2025: First-of-Its-Kind Production Deployments —** While there will be thousands of generic agents in the market soon, it will take some time before we see something real and in production. While the demos for building agents make things look super easy, there's going to be a lot of IT and governance work needed before we see things graduate from the sandbox. But by this time next year we will see real progress from real customers.

What Are The Challenges For AI Agents?

Application platforms have a major time-to-market advantage for agents and will be an excellent vector for deploying internal agents, provided that the platform has good rules and data structures. That said, scalability, management and governance are major considerations when it comes to high-scale deployments.

Governance — The specificity and context of agents will likely come from internal enterprise information. However, the data that the model or agent will use will need to be appropriately secured and have policies applied before it can be used. So, grounding the agents with the right data will be paramount for managing risk.

AI Agents Will Be The Key To Achieving ROI From AI

Testing — How will an agent be tested? It's one thing to create an automated testing scheme for a deterministic application. But LLMs are not deterministic at all, and the same prompt may deliver a different result at different times. What should testing look like, and what will be the best practices? And of course there are considerations for performance, latency and user experience as well.

Observability — How the various agents will be managed and measured will be an enormous task. This is about determining not only the right things to monitor, but also the right expectations one should have of an agent. For instance, it's nice to know that the agent answered 50 client requests in a day—but did that improve or impair customer satisfaction?

Performance and Efficiency — Any process re-engineering effort, whether human or machine-based, is bound to find new bottlenecks or items that weren't considered. The ideas that workers have in their heads thanks to years of experience may very well deviate from what was documented five years ago. To take another example, when the new agents start hitting the credit-check API five times faster than humans, your performance or costs may change. Thorough testing of the process via a rigorous pilot is mandatory.

What Should Enterprises Do In The Next 12 Months?

Despite these challenges, enterprises should start working with AI agents as soon as possible to understand how they can inform organizational strategy. Here are three specific recommendations.

AI Agents Will Be The Key To Achieving ROI From AI

Walk before you run. If you are a user of an application platform, I'd start there because there are many components and lots of meaningful data in place. However, the first rollout should be a team-focused pilot so that organizational and technical gaps can be understood before a larger rollout.

Designate a "general manager of agents." Agents are a new type of workforce, so to speak, and there needs to be a C-level owner responsible for that workforce. There will be many organizational learnings that come from deploying agents, which are not like most other applications or processes. The "GM of agents" will need to track these learnings and touch many parts of the organization to simultaneously advocate and manage risk in the context of the emerging business reality.

Stretch out testing as much as possible. There are not a lot of best practices established in this space, so testing will be crucial. Learning what to expect in terms of the technology, user acceptance and what's needed to scale will all be massive inputs for how the organization will measure the success of any AI program.

Conclusion

AI-based agents will go a long way towards helping organizations understand the potential and actual impact of AI-based technologies. Additionally, the ability to leverage organization-specific data and services will enable AI agents to operate more precisely and add more value. The level of practicality and reduced risk in deploying AI agents alongside application platforms such as Salesforce or ServiceNow may be the entry point most CXOs have needed to start investing.