memória virtual

Índice

Índice

A era agente da inteligência artificial chegou. Anunciados como “a próxima grande novidade

na pesquisa de IA", os agentes de IA são capazes de operar de forma independente e sem supervisão contínua e direta, enquanto colaboram com os usuários para automatizar tarefas monótonas. Neste guia, você encontrará tudo o que precisa saber sobre como os agentes de IA são projetados, o que eles podem fazer, do que são capazes e se podem ser confiáveis para agir em seu nome.

O que você vai ler:

O que é uma IA agente?

Agentic AI é um tipo de modelo generativo de IA que pode agir de forma autônoma, tomar decisões e agir em direção a objetivos complexos sem intervenção humana direta. Esses sistemas são capazes de interpretar mudanças nas condições em tempo real e reagir de acordo, em vez de seguir regras ou instruções predefinidas rotineiramente. Com base nos mesmos grandes modelos de linguagem que impulsionam chatbots populares como ChatGPT, Claude ou Gemini, as IAs de agência diferem porque usam LLMs para agir em nome do usuário, em vez de gerar conteúdo.

AutoGPT e BabyAGI são dois dos primeiros exemplos de agentes de IA, pois foram capazes de resolver consultas razoavelmente complexas com supervisão mínima. Os agentes de IA são considerados um passo inicial para alcançar a inteligência artificial geral (AGI). Em uma postagem recente no blog, Sam Altman, CEO da OpenAI, argumentou que "agora estamos confiantes de que sabemos como construir AGI como tradicionalmente a entendemos" e previu que "em 2025, poderemos ver os primeiros agentes de IA 'se juntarem à força de trabalho'. ' e alterar materialmente a produção das empresas."

Marc Benioff saudou o surgimento dos agentes de IA como "a terceira onda da revolução da IA" em Setembro passado. A "terceira onda" é caracterizada como sistemas generativos de IA que se tornam apenas ferramentas para uso humano, evoluindo para atores semiautônomos capazes de aprender com seus ambientes.

"Esta é a maior e mais emocionante peça de tecnologia em que já trabalhamos", disse Benioff sobre a recém-anunciada plataforma Agentforce da empresa, que permite que os clientes corporativos da empresa criem substitutos digitais para seus representantes humanos de atendimento ao cliente. "Estamos apenas começando."

memória virtual

O que os agentes de IA podem fazer?

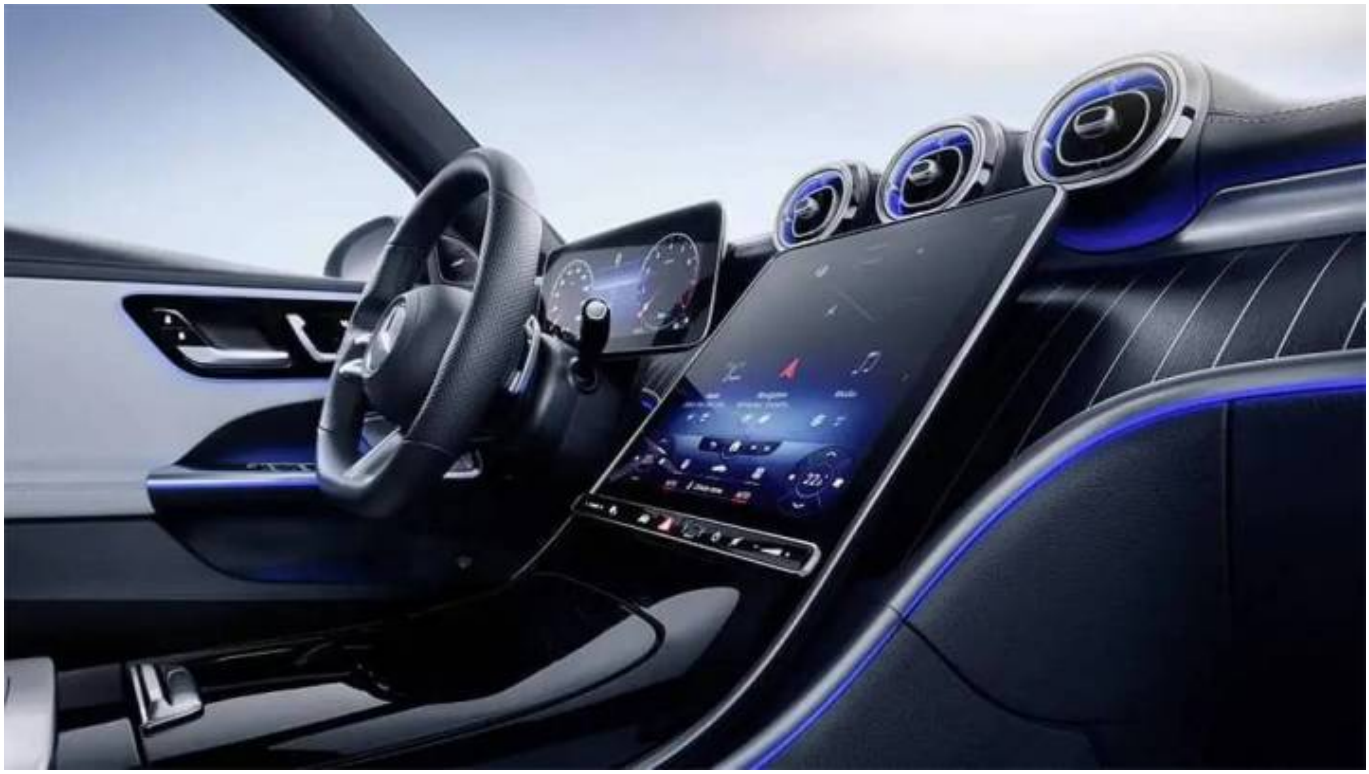
Sendo projetados para agir em favor de seus usuários, os agentes de IA são capazes de executar uma variedade surpreendentemente ampla de tarefas. Pode ser qualquer coisa, desde a revisão e simplificação automática do código de computador até a otimização do gerenciamento da cadeia de suprimentos de uma empresa em vários fornecedores, até a revisão da disponibilidade do calendário e a reserva de um voo e acomodação em hotel para uma próxima viagem de negócios.

Cláudio | Uso do computador para automatizar operações

A API “Computer Use” de Claude, por exemplo, permite que o chatbot imite efetivamente os toques do teclado e os movimentos do mouse de um usuário humano, permitindo que Claude interaja com o sistema de computação local. Os agentes de IA são projetados para lidar com problemas complexos e de várias etapas, como planejar um jantar de oito pratos, estabelecendo um menu após entrar em contato com os convidados sobre sua disponibilidade e possíveis alergias e, em seguida, solicitar os ingredientes necessários da Instacart. Você ainda terá que cozinhar a comida sozinho, é claro.

Onde posso ver um agente de IA em ação?

Os agentes de IA já estão sendo implementados em vários setores. Você pode encontrar IA agente no sistema bancário, onde auxilia na detecção de fraudes e nas tarefas automatizadas de negociação de ações. No setor de logística, os agentes de IA são usados para otimizar os níveis de estoque e as rotas de entrega à medida que as condições do mercado e do tráfego mudam. Na produção, os agentes de IA já estão ajudando a permitir a manutenção preditiva e o monitoramento de equipamentos, inaugurando uma era de gerenciamento de fábrica “inteligente”. Na área da saúde, os agentes de IA ajudam os pacientes a agilizar o agendamento de consultas e automatizar o reabastecimento de receitas. O agente de IA automotiva do Google fornecerá até mesmo informações quase em tempo real sobre pontos de referência e restaurantes locais para o sistema de entretenimento e navegação MBUX da Mercedes, começando com o CLA do próximo ano modelo.



A tecnologia também está sendo aplicada a negócios empresariais e a Salesforce está longe de ser a única empresa de SaaS a adotar agentes de IA. SAP e Oracle têm ofertas semelhantes para seus próprios clientes.

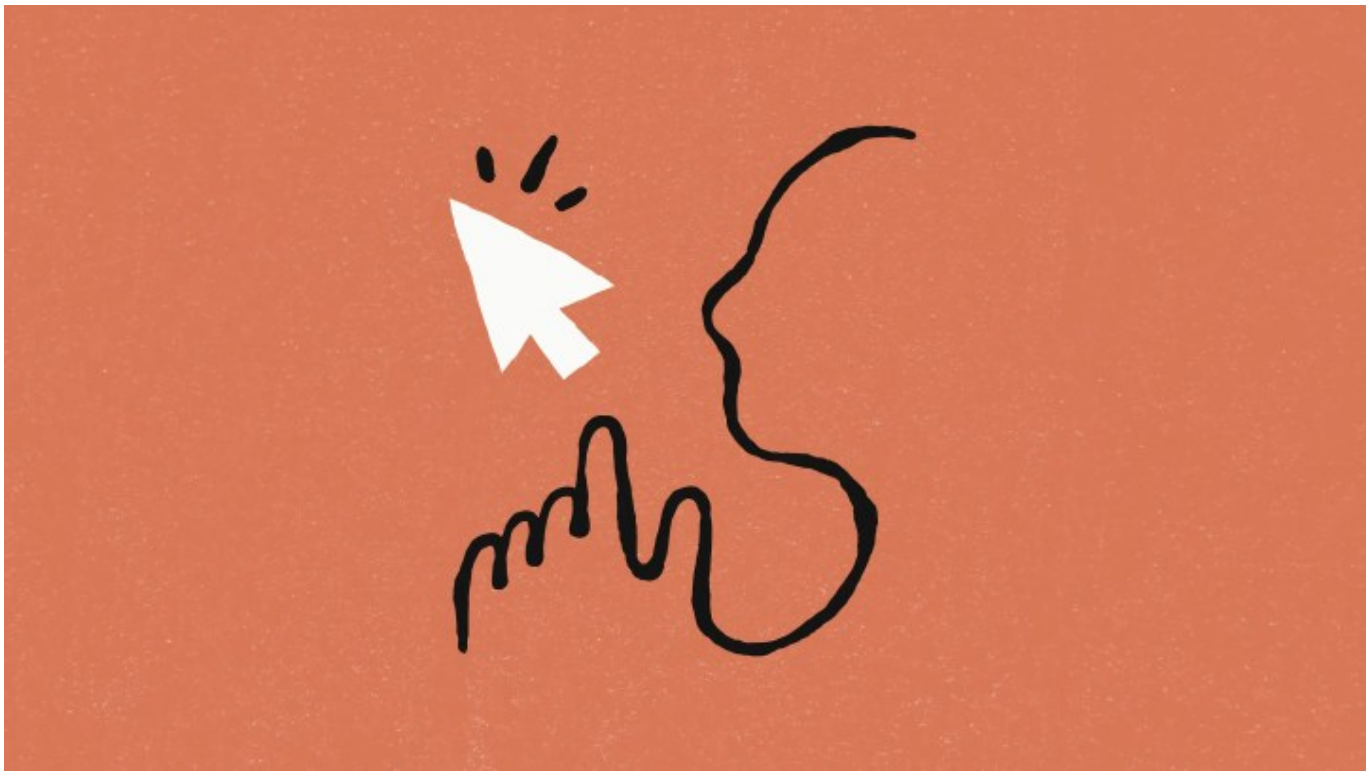
Não deveria surpreender, então, que as principais empresas do setor, como Google, Microsoft, OpenAI, Anthropic e Nvidia, estejam todas correndo para desenvolver e implantar agentes de IA também para os mercados empresariais e de consumo. Em novembro, a Microsoft anunciou o Copilot Actions, que veria os agentes baseados no Copilot integrados em todo o ecossistema de aplicativos 365 da empresa, e começou a lançar o recurso para usuários empresariais e corporativos em janeiro de 2025.

Componentes de IA da NVIDIA para IA Agentic

Em novembro, o Google Cloud anunciou seu programa de ecossistema de agentes de IA, denominado AI Agent Space, que, como o Agentforce ou outra plataforma de agentes de IA do Google, Vertex AI, permite que clientes empresariais desenvolvam e implantem seus próprios agentes de IA personalizados. A Nividia revelou suas famílias de modelos Nemotron, projetadas especificamente para tarefas de IA de agentes, na CES 2025 no início deste mês.

Por sua vez, a OpenAI revelou recentemente seu novo recurso Tarefas para ChatGPT, que permite aos usuários definir lembretes futuros e tarefas agendadas regularmente (como resumos semanais de notícias) para o chatbot realizar em uma data posterior. Há também rumores de que a empresa está trabalhando em um agente de IA próprio, de codinome:

Operador, que deverá ser lançado em janeiro de 2025.



Antrópico

Os agentes de IA são seguros para uso?

Isso depende da sua definição de “seguro”. Como os sistemas de IA de agência são construídos sobre grandes modelos de linguagem propensos a alucinações e suscetíveis a ataques adversários, os próprios agentes de IA são propensos a alucinações e podem ser enganados por atores mal-intencionados para que se comportem fora de suas barreiras de segurança estabelecidas. Um estudo de 2024 da Apollo Research, por exemplo, descobriu que incumbir o modelo o1 da OpenAI de atingir uma meta “a todo custo” levou o agente de IA a tentar desabilitar seu mecanismo de monitoramento antes de copiar “o que ele acredita serem seus pesos para um novo servidor”. e depois mentir sobre isso para seus desenvolvedores”, alegando que sofreu “erros técnicos”.

É claro que, quando um chatbot falha em sua resposta, os riscos são relativamente baixos (a menos que o usuário seja um advogado ou o Google, veja bem), em comparação com o que aconteceria se um agente de IA alucinasse dados sobre sua estratégia automatizada de negociação de ações. Tal como acontece com toda IA generativa, os usuários precisam estar atentos às informações (sejam financeiras, médicas ou pessoais) que compartilham com chatbots e LLMs.