

☐☐ Nuovo ChatGPT Agente: ora ragiona, decide e agisce da solo

Maria Cattini | 25/07/2025 | Intelligenza Artificiale

ChatGPT agente: cosa può fare davvero

☐☐ Il 17 luglio 2025 segna un nuovo capitolo **ChatGPT diventa un agente attivo**. Non solo scrive, ora agisce. Può navigare il web, interagire con siti, compilare fogli di calcolo, generare presentazioni, e persino automatizzare attività complesse, tutto in autonomia. Il salto è netto: da assistente passivo a **collaboratore operativo**.

Il nuovo sistema agentico consente a ChatGPT di:

- Interagire con browser visivi e testuali
- Accedere e usare API
- Scrivere codice in un terminale virtuale
- Scegliere autonomamente lo strumento più adatto al compito

Tutto questo **su un computer virtuale integrato**, che conserva il contesto e coordina i passaggi.

Esempio concreto: può analizzare i tuoi concorrenti, creare una presentazione con grafici, e sintetizzare i risultati in un file pronto all'uso. Tu dai l'input, ChatGPT fa il resto.

☐☐ Come si attiva la modalità agente

Per gli utenti **Pro, Plus e Team**, è già possibile attivare il sistema:

- dal menu a discesa nel compositore di messaggi
- selezionando "modalità agente"

Il sistema richiede **sempre l'autorizzazione** prima di agire, e puoi interrompere l'attività in qualsiasi momento.

☐☐ Cosa può fare ChatGPT agente

☐☐ In ambito lavorativo

- Riprogrammare meeting e creare agende personalizzate
- Compilare fogli di calcolo aggiornando dati
- Generare presentazioni da dati grezzi
- Fare scraping e sintesi di siti web per analisi di mercato

☐☐ Nella vita quotidiana

- Pianificare cene e prenotare ristoranti
- Organizzare viaggi completi (voli, hotel, itinerari)
- Trovare specialisti e fissare appuntamenti

☐☐ Ricerca intelligente

Integra tre capacità distinte:

- Navigazione web (Operator)
- Analisi e sintesi approfondita (Deep Research)
- Conversazione fluida e personalizzata (ChatGPT)

☐☐ Benchmark: dove supera gli umani

Secondo i dati ufficiali, l'agente ChatGPT ha:

- superato modelli precedenti nei test Humanity's Last Exam
- ottenuto il 44,4% di accuratezza grazie a una strategia multi-tentativo
- superato i competitor nei test di data science e modifica fogli di calcolo

Nel benchmark SpreadsheetBench ha raggiunto il **45,5%** contro il 20% di Copilot su Excel.

☐☐ Sicurezza: nuovi poteri, nuovi rischi

Con il potere arriva la responsabilità. Per questo sono stati introdotti:

- Conferme esplicite prima di ogni azione sensibile
- Modalità supervisione per attività delicate come l'invio email
- Rifiuto automatico di compiti ad alto rischio (es. bonifici bancari)
- Protezione da prompt injection (istruzioni malevole nascoste nei siti)
- Controllo privacy totale: puoi cancellare tutto con un clic

☐☐ Biosicurezza: il nuovo standard

L'agente è stato trattato come un sistema ad **alta capacità biologica**, con uno dei più avanzati stack di sicurezza mai implementati da OpenAI. Include:

- Test in scenari reali
- Collaborazioni con esperti di biosicurezza
- Simulazioni per evitare l'uso improprio della tecnologia

☐☐ Chi può usarlo (e quando)

- Già attivo per utenti Pro
- In arrivo per Plus e Team
- Accesso previsto per Enterprise e Education
- 400 messaggi/mese per i Pro, 40 per gli altri (con crediti aggiuntivi)

⚠ Attualmente non disponibile nello Spazio Economico Europeo e in Svizzera.

☐☐ Limitazioni note

- La creazione di presentazioni è ancora in fase beta
- Alcuni output esportati possono risultare grezzi
- Non tutti i flussi sono ancora perfettamente fluidi

📄 Cosa ci aspetta

OpenAI ha confermato che continuerà:

- ad ampliare le capacità dell'agente
- a migliorare la fluidità delle interazioni
- a ridurre la supervisione necessaria, mantenendo la sicurezza

📄 In sintesi

Funzionalità	Dettagli
Browser visivo	Navigazione e interazione come un utente umano
Browser testuale	Analisi veloce di contenuti complessi
Terminale	Esecuzione di codice per analisi o trasformazioni
Accesso API	Integrazione con app come Gmail, GitHub, Google
Contesto persistente	Mantiene i dati tra strumenti e passaggi
Supervisione	Sempre sotto il controllo dell'utente
Sicurezza potenziata	Protezioni contro uso improprio e fughe di dati

📄 Vuoi provare il nuovo ChatGPT agente?

📄 Attiva la modalità agente dal menu degli strumenti e dai un comando come:

“Prepara una presentazione sui miei competitor”

oppure

“Controlla il calendario e prenota una cena giapponese per 4”

Fatto? Raccontaci come ti sei trovato!

ChatGPT agente: cosa può fare davvero

📄 Il 17 luglio 2025 segna un nuovo capitolo **ChatGPT diventa un agente attivo**. Non solo scrive, ora agisce. Può navigare il web, interagire con siti, compilare fogli di calcolo, generare presentazioni, e persino automatizzare attività complesse, tutto in autonomia. Il salto è netto: da assistente passivo a **collaboratore operativo**.

Il nuovo sistema agentico consente a ChatGPT di:

- Interagire con browser visivi e testuali
- Accedere e usare API
- Scrivere codice in un terminale virtuale
- Scegliere autonomamente lo strumento più adatto al compito

Tutto questo **su un computer virtuale integrato**, che conserva il contesto e coordina i passaggi.

Esempio concreto: può analizzare i tuoi concorrenti, creare una presentazione con grafici, e sintetizzare i risultati in un file pronto all'uso. Tu dai l'input, ChatGPT fa il resto.

☐☐ Come si attiva la modalità agente

Per gli utenti **Pro, Plus e Team**, è già possibile attivare il sistema:

- dal menu a discesa nel compositore di messaggi
- selezionando “modalità agente”

Il sistema richiede **sempre l'autorizzazione** prima di agire, e puoi interrompere l'attività in qualsiasi momento.

☐☐ Cosa può fare ChatGPT agente

☐☐ In ambito lavorativo

- Riprogrammare meeting e creare agende personalizzate
- Compilare fogli di calcolo aggiornando dati
- Generare presentazioni da dati grezzi
- Fare scraping e sintesi di siti web per analisi di mercato

☐☐ Nella vita quotidiana

- Pianificare cene e prenotare ristoranti
- Organizzare viaggi completi (voli, hotel, itinerari)
- Trovare specialisti e fissare appuntamenti

☐☐ Ricerca intelligente

Integra tre capacità distinte:

- Navigazione web (Operator)
- Analisi e sintesi approfondita (Deep Research)
- Conversazione fluida e personalizzata (ChatGPT)

☐☐ Benchmark: dove supera gli umani

Secondo i dati ufficiali, l'agente ChatGPT ha:

- superato modelli precedenti nei test Humanity's Last Exam
- ottenuto il 44,4% di accuratezza grazie a una strategia multi-tentativo
- superato i competitor nei test di data science e modifica fogli di calcolo

Nel benchmark SpreadsheetBench ha raggiunto il **45,5%** contro il 20% di Copilot su Excel.

☐☐ Sicurezza: nuovi poteri, nuovi rischi

Con il potere arriva la responsabilità. Per questo sono stati introdotti:

- Conferme esplicite prima di ogni azione sensibile
- Modalità supervisione per attività delicate come l'invio email
- Rifiuto automatico di compiti ad alto rischio (es. bonifici bancari)
- Protezione da prompt injection (istruzioni malevole nascoste nei siti)
- Controllo privacy totale: puoi cancellare tutto con un clic

🔒 Biosicurezza: il nuovo standard

L'agente è stato trattato come un sistema ad **alta capacità biologica**, con uno dei più avanzati stack di sicurezza mai implementati da OpenAI. Include:

- Test in scenari reali
- Collaborazioni con esperti di biosicurezza
- Simulazioni per evitare l'uso improprio della tecnologia

👤 Chi può usarlo (e quando)

- Già attivo per utenti Pro
- In arrivo per Plus e Team
- Accesso previsto per Enterprise e Education
- 400 messaggi/mese per i Pro, 40 per gli altri (con crediti aggiuntivi)

⚠ Attualmente non disponibile nello Spazio Economico Europeo e in Svizzera.

📝 Limitazioni note

- La creazione di presentazioni è ancora in fase beta
- Alcuni output esportati possono risultare grezzi
- Non tutti i flussi sono ancora perfettamente fluidi

🔮 Cosa ci aspetta

OpenAI ha confermato che continuerà:

- ad ampliare le capacità dell'agente
- a migliorare la fluidità delle interazioni
- a ridurre la supervisione necessaria, mantenendo la sicurezza

📋 In sintesi

Funzionalità	Dettagli
Browser visivo	Navigazione e interazione come un utente umano
Browser testuale	Analisi veloce di contenuti complessi
Terminale	Esecuzione di codice per analisi o trasformazioni
Accesso API	Integrazione con app come Gmail, GitHub, Google
Contesto persistente	Mantiene i dati tra strumenti e passaggi
Supervisione	Sempre sotto il controllo dell'utente
Sicurezza potenziata	Protezioni contro uso improprio e fughe di dati

👤 Vuoi provare il nuovo ChatGPT agente?

👤 Attiva la modalità agente dal menu degli strumenti e dai un comando come:

“Prepara una presentazione sui miei competitor”

oppure

“Controlla il calendario e prenota una cena giapponese per 4”

Fatto? Raccontaci come ti sei trovato!