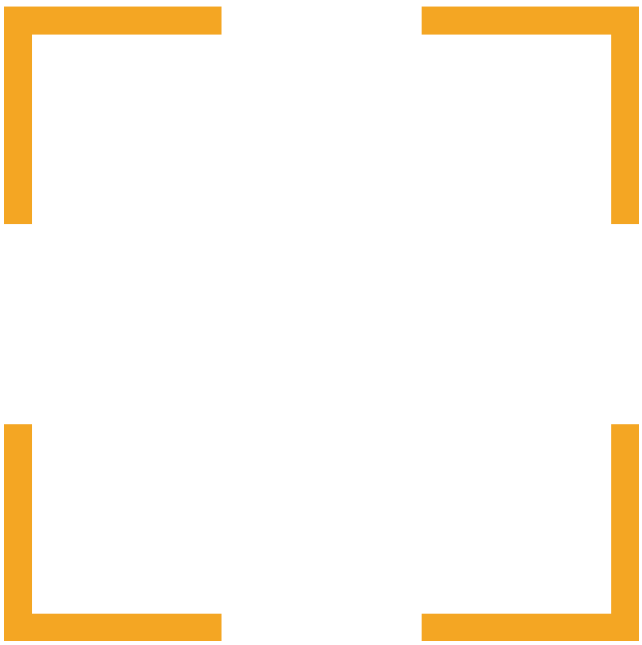
GUNPOWDER

WHITE PAPER · MAGGIO 2026

Dall'agent-washing all'Agentic Enterprise

Oltre il boom della Generative AI: l'orchestrazione agentica delle aziende italiane nel 2026

Ti interessa avere questo documento
in versione **podcast o digitale**?



GUNPOWDER

INDICE

Sommario

GUNPOWDER

01

CAPITOLO 1

Dove siamo nel percorso verso l'Agentic Enterprise

1.0 Un normale venerdì mattina agentico

È una mattina di maggio 2026, le sette e quattordici di venerdì. Sulla casella di posta elettronica di un'azienda italiana di componentistica industriale, arriva un'email da un cliente storico: chiede di riconfigurare l'ordine annuale alla luce di un cambio di mix produttivo, e vuole la proposta per lunedì.

Nessuno è ancora in ufficio, ma l'email viene aperta da qualcuno. O meglio, da qualcosa.

Un agente AI legge il messaggio, lo classifica come "modifica ordine con impatto plan", incrocia in autonomia lo storico delle forniture, lo stato delle scorte sui codici coinvolti, le previsioni di domanda dei prossimi quattro mesi, le condizioni contrattuali in vigore.

Prepara tre opzioni di riconfigurazione, calcola la simulazione di consegna per ciascuna, redige la bozza di proposta in PDF. Su due voci minori applica direttamente le modifiche secondo i parametri pre-autorizzati nel contratto quadro: lo sconto di fascia A in vigore dal primo trimestre, la cadenza di consegna mensile preferita dal cliente. Sui restanti, segnala alla sala procurement gli elementi che richiedono ratifica umana, con la nota tecnica accanto a ognuno.

Alle nove, quando il team procurement arriva in ufficio, trova sulla scrivania, o meglio sul desktop, tre documenti pronti e un riepilogo decisionale di mezza pagina. Sette minuti di lavoro dell'agente, che hanno fatto risparmiare l'equivalente di una mattinata di lavoro umano.

Questo non è il futuro, è il presente. O quantomeno potrebbe esserlo.

Ma allora perché così poche aziende possono ancora dire che questo sia uno scenario realistico di un normale venerdì mattina?

I dati più recenti sull'adozione dell'AI raccontano di una corsa globale e di una zoppia italiana, e per capirli vanno letti insieme.

Si parla moltissimo di agenti AI e dell'impatto che avranno sul mondo del lavoro e sulla produttività delle aziende. L'hype nei confronti di questa tecnologia è altissimo, e si moltiplicano i vendor di soluzioni sedicenti "agentiche". Eppure i risultati, se arrivano, sono spesso sotto le aspettative e le promesse.

Capire dove finisce la narrativa commerciale e dove cominciano le vere potenzialità diventa sempre più difficile.

E così molte aziende restano in attesa, indecise su come partire e cosa fare nel concreto. E più passa il tempo, più diventa difficile fare quel primo passo che sembra ingigantirsi.

Tante altre partono di fretta, spinte dal timore di restare indietro, in modo un po' casuale, senza una governance chiara e una visione realistica di dove vogliono arrivare. E come succede in molti processi legati all'AI, dove ogni step è esponenziale, si trovano a gestire processi che non scalano o che non portano i benefici attesi. A volte peggiorando addirittura la situazione di partenza.

Queste situazioni sono motivate da due elementi interconnessi. Il primo è una questione di numeri: anche se l'hype attorno agli agenti AI è altissimo, dai dati emerge che la quota di chi ha messo in produzione agenti veri è ancora bassa.

Il secondo è di definizioni: molti chiamano agentic enterprise e agenti qualcosa che non lo è, e questo è un equivoco caro, perché orienta budget, roadmap e aspettative su un'idea sbagliata dell'opportunità.

Fare chiarezza su questi aspetti, per capire come muoversi con metodo e consapevolezza, è l'obiettivo di queste pagine.

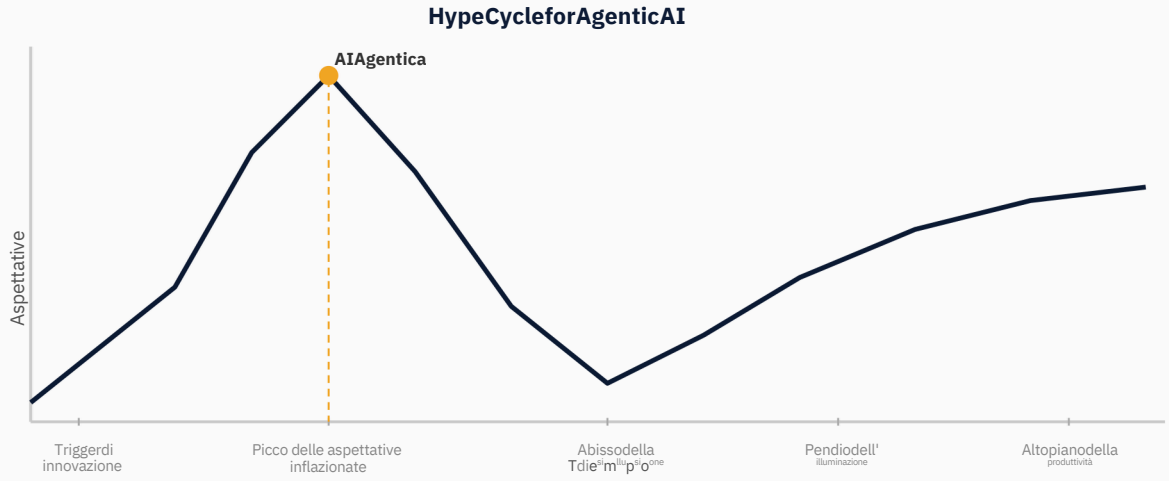
La corsa globale.

L'Hype Cycle for Agentic AI 2026 di Gartner, pubblicato a metà aprile, fotografa la curva di adozione più aggressiva mai misurata su una categoria emergente, con "solo il 17% delle organizzazioni che ad oggi ha messo in produ-

1.1 I numeri che spiegano il divario

zione agenti AI, ma oltre il 60% che conta di farlo nei prossimi due anni" (Gartner, What the 2026 Hype Cycle for Agentic AI Reveals). Nessuna tecnologia dell'ultimo decennio ha mostrato un'aspettativa di adozione così ra- pida.

Ma, nella stessa pubblicazione, Gartner colloca l'*Agentic AI* esattamente sul **Peak of Inflated Expectations**, cioè la fase in cui le aspettative superano le capacità concrete della tecnologia. Ciò significa che chi si affretta ad arrivare per primo, saltando le tappe, rischia di trovarsi in mano solo disillusione.



Fonte: Gartner,Whatthe 2026 Hype Cycle for AgenticAI Reveals

Tuttavia, la corsa è necessaria: i miglioramenti delle capacità dell'AI si sono già dimostrati imprevedibilmente rapidi, e la tecnologia alla base degli Agenti è già matura. L'importante è iniziare a muoversi, con ordine e consape- volezza dell'obiettivo, perché restare indietro in questo momento può essere irreversibile.

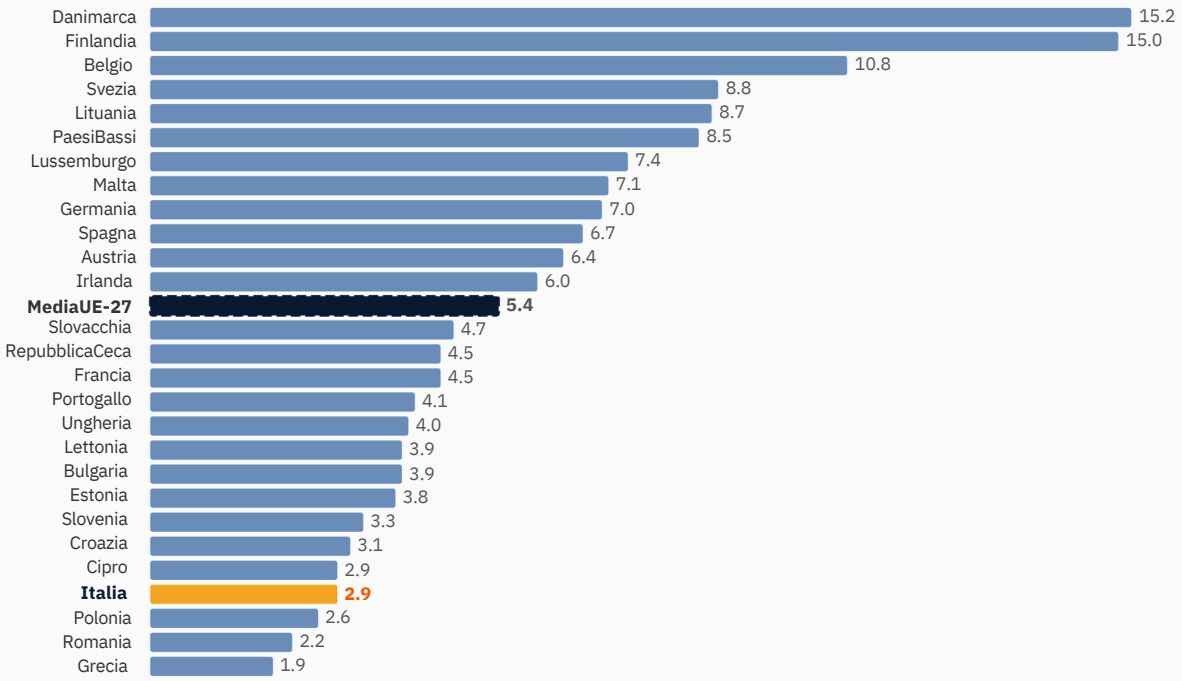
La zoppia italiana.

Il mercato dell'AI in Italia valeva 1,8 miliardi di euro nel 2025, in crescita del 50% sull'anno precedente, con un tasso composto triennale del 54% (Osservatorio Artificial Intelligence, Politecnico di Milano, *Artificial Intelligence nel 2025: mercato, adozione e trasformazione delle aziende*, pag. 7-8). Su questi 1,8 miliardi, la Generative AI da sola pesa il 46% del totale e cresce del 60% in un anno, più del doppio del ritmo del mercato AI complessivo. È il segmento che sta trainando la crescita.

Al contrario, i sistemi di **Process Orchestration e Agentic AI** valgono ancora solo il 4% del mercato italia- no, una quota marginale. Il salto agentico, insomma, è iniziato anche in Italia, ma su una base molto piccola.

Il ritardo si misura anche nel confronto europeo. Su dati Eurostat 2024 elaborati da TEHA Group, in Italia il 2,9% delle imprese ha dichiarato di utilizzare tecnologie di IA Agentica, contro il 4,5% della Francia, il 6,7% della Spagna e oltre il 7,0% della Germania (Ambrosetti / Microsoft, *AI Skills 4 Agents Observatory*, settembre 2025).

Aziende che utilizzanol'IA Agentica neiPaesiUE(% sultotale),2025



Fonte: elaborazioneTEHA Group su dati Eurostat,2026. Da Ambrosetti /Microsoft, AI Skills Agents Observatory, settembre2025.

Un altro dato può aiutarci a capirne il motivo. Il 71% delle grandi imprese italiane ha avviato almeno una progettualità AI nel 2025, in crescita dal 59% del 2024; di queste, l'84% ha almeno un'iniziativa di Generative AI (96% tra le grandissime aziende). Eppure **soltanto il 9% dichiara di avere una governance AI integrata e matura** (Osservatorio AI PoliMi, pag. 15, 16, 23) a sostenere questi progetti.

È un Paese che, per la maggior parte, ha comprato gli strumenti, ma non ha ancora deciso chi li userà, con quali regole e dentro quali processi.

Il nuovo washing da cui proteggersi.
C'è un termine che sta diventando sempre più popolare per descrivere il gap tra promesse di vendita e reale portata degli agenti AI.

Si chiama **agentwashing**, ovviamente. L'Osservatorio Intelligent Business Process Automation del Politecnico di Milano, nel report 2026 *Process Intelligence & Automa- tion in Italia*, ha documentato proprio questo fenomeno.

Il 62% delle grandi imprese italiane non conosce l'argomento o non ha avviato attività su Agentic Automation.

Fra le imprese interessate, invece, il 25% è in fase di analisi, **il 13% ha avviato sperimentazioni**. Ma di quel 13%, **solo l'8% riconosce nelle proprie soluzioni le caratteristiche distintive dell'Agentic Automation**.

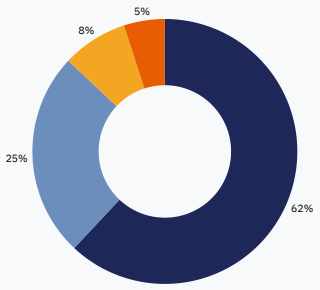
Il restante 5% afferma di averla introdotta, ma descrive semplicemente un workflow AI (Osservatorio IBPA Politecnico di Milano, *Process Automation in Italia*).

Quando le imprese vengono poi interrogate su quali caratteristiche associano all'Agentic Automation, in testa alla classifica mettono *"interazione conversazionale"* (21%), *"generazione di contenuti"* (21%) e *"supporto tramite raccomandazioni"* (19%). Le capacità realmente distintive di un sistema agentico, cioè **autonomia operativa e orientamento agli obiettivi**, sono invece in fondo all'elenco, intorno al 9-10%.

Le aziende, insomma, dichiarano spesso di essere agentiche senza esserlo. E lo fanno perché hanno in mente il concetto sbagliato.

Process Intelligence & Automation—dove sitrovanole aziende italiane nel2025

GRADO DI ADOZIONE DELL'AGENTIC AUTOMATION



- 62%— Aziende che non hanno avviato sperimentazioni in ambito Agentic Automation
- 25%— Aziende in fase di analisi delle potenzialità
- 8% — Aziende che hanno avviato sperimentazioni
- 5%—Aziende che pensano di avere soluzioni agentiche quando in realtà ciò che descrivono sono soluzioni AI Workflow

CARATTERISTICHE ASSOCIATE ALL'AGENTIC AUTOMATION

Interazioneconversazionale	21%
Generazionedi contenuti	21%
Supportotramiteraccomandazioni	19%
Collaborazioneeadattamentomulti-agente	17%
Accessoamemoriaeapprendimentocontinuo	16%
Usodi strumenti (tool usage)	16%
Esecuzionedi flussi di lavoropredefiniti	12%
Autonomia operativa	**10%**
Orientamento agli obiettivi	**9%**
Nonhoabbastanzainformazioni	2%

Fonte: Osservatorio Intelligent Business Process Automation, Politecnico di Milano

1.2 L'obiettivo del documento

Questo documento si propone di essere l'antidoto all'agentwashing e alla confusione informativa dilagante. Per riuscirci, è necessario partire dalle basi, chiarendo definizioni e perimetri di utilizzo del termine.

Il capitolo 2 lavora su questo. Disegna una mappa minima dell'AI del 2026, distingue la capability dal sistema, e definisce con precisione cos'è un'agentic enterprise.

Il capitolo 3 descrive un approccio pragmatico e sequenziale di implementazione dell'AI verso l'Agentic Enterprise, e lo fa attraverso tre storie italiane. Tre casi reali, che rappresentano bene tre gradini diversi che ogni azienda deve superare, quando prova a passare dall'intenzione alla produzione.

Il capitolo 4 disegna una matrice a due assi (sovranità del dato × ecosistema vendor) con quattro quadranti, una griglia informativa per scegliere il mix giusto fra le opzioni architetturali disponibili oggi sul mercato.

Il capitolo 5, infine, guarda avanti, per ipotizzare dove sta andando il mercato nei prossimi dodici-diciotto mesi, e cosa occorre iniziare a mettere a terra prima che sia tar- di.

A scriverlo è una società italiana, Salesforce Partner Summit dal 2017, con oltre 400 progetti realizzati in più di dieci industrie, che lavora su questi cantieri tutti i giorni. Che ha seguito i go-live, gestito le crisi, raccolto i KPI dopo la stabilizzazione, visto da vicino cosa succede quando un agente esce dalla sandbox e diventa la quoti- dianità.

E che da questa prospettiva privilegiata può offrire una lettura utile alle imprese che vogliono capire dove sono, dove devono andare, e come arrivarci senza sprecare risorse e tempo prezioso.

GUNPOWDER

02

CAPITOLO 2

Fare chiarezza sull'Agentic Enterprise

2.0 Una mappa dell'AI per orientarsi

Agentic enterprise, termine che dà il titolo a questo documento, è un concetto molto evocativo e ricco di promes- se. Allo stesso tempo, è forse anche il termine più ambiguo del lessico tech del 2026.

Tra i due fatti c'è un legame, ed è il motivo di questo capitolo: senza parole chiare, l'agentic rischia di essere uno specchietto per le allodole di massa.

Per orientarsi nel rumore lessicale del momento, basta una mappa minima. Le sigle dell'AI di cui si parla maggiormente nel 2026 si possono ricondurre infatti a tre categorie di funzioni.

- L'**AI predittiva**, modelli di machine learning addestrati su dati storici, prevede (anomalie, picchi di domanda, guasti di un macchinario, frodi).
- L'**AI generativa**, large language model che producono output, produce (testo, codice, sintesi, immagini, traduzioni).
- L'**AI agentica**, sistemi che orchestrano strumenti per raggiungere un obiettivo, decide e agisce.

Predittiva e generativa sono *capability*. Stanno dentro fogli Excel, copilot, sistemi RPA, dashboard di anomaly detection. Si comprano, si integrano, si usano puntualmen- te.

L'agentica è invece un sistema: non sostituisce le prime due, le usa come strumenti.

Un esempio può aiutare a chiarire meglio la distinzione. Immaginiamo un agente di customer service che riceve la richiesta “perché la mia ultima bolletta è più alta della precedente?”. Per rispondere, l'agente consulta in autonomia un modello predittivo, che identifica eventuali anomalie nei consumi del cliente, interroga un modello generativo per redigere la risposta personalizzata, scrive nel CRM la nota di follow-up.

La capacità predittiva e quella generativa sono gli ingredienti della risposta, l'agente è il cuoco.

L'Osservatorio Intelligent Business Process Automation del Politecnico di Milano formalizza una mappa simile, in maggiore dettaglio. Distingue sei sottoinsiemi di utilizzo dell'AI nell'automazione di processo digitale:

1. Conversational RPA (agenti conversazionali con Robotic Process Automation)
2. Intelligent Document Processing (processi di estrazione e comprensione di informazioni da documenti non strutturati)
3. Logiche decisionali dinamiche e predittive (algoritmi di machine learning che analizzano dati storici e prevedono risultati futuri)
4. Coordinamento intelligente di processi (AI che coordina processi tra sistemi diversi, ad esempio tra ERP e CRM)
5. Simulazione e pianificazione automatizzata (AI che simula scenari e pianifica azioni in base a dati storici e in tempo reale)
6. L'ultima voce, l'Agentic Automation, è quasi una categoria a sé, perché non è una capability di automazione, è il sistema che le orchestra.

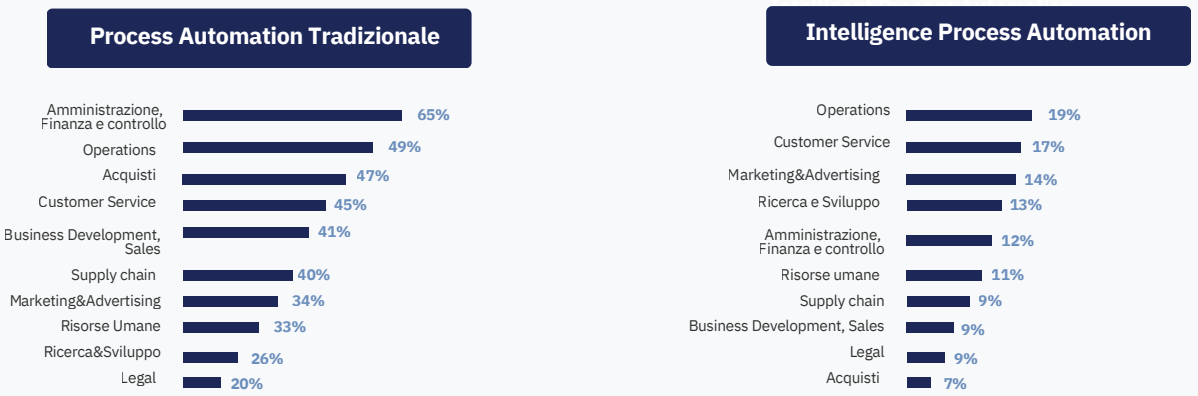
Un LLM (Large Language Model) che sfrutta le capacità di comprensione e generazione linguistica per dirigere un processo dinamico, multi-step e multi-piattaforma, assumendo decisioni che combinano ragionamento, memoria e pianificazione.

Definita la mappa, emerge chiara la causa della confusio- ne, involontaria o dovuta al processo di agentwashing, vista nel capitolo precedente.

Il 5% di imprese italiane che dichiara di fare Agentic Automation ma descrive un workflow AI fa confusione fra capability e sistema: pensa che avere un modello generati- vo integrato dentro un processo automatizzato sia un agente.

Non lo è.

La presenza di applicazioni di Process Automation nelle funzioni aziendali (2025)



Fonte: Osservatorio Intelligent Business Process Automation, Politecnico di Milano.

2.1 Tre tipi di sistemi che vengono chiamati “agentic”

Tre famiglie di sistemi vengono oggi chiamate “agentic” indistintamente, spesso anche a torto. Vediamole in ordine di autonomia crescente.

Copilot e chatbot di assistenza

L'AI risponde, redige, suggerisce, sintetizza. L'umano è nel loop a ogni passaggio: chiede, riceve, valuta e agi- sce. Microsoft 365 Copilot, ChatGPT come assistente, Claude come collaboratore di scrittura.

L'AI utilizzata in questo modo ha un limite strutturale: non esegue azioni in autonomia. Migliora la produttività individuale di chi la usa, ma non trasforma un processo aziendale. Non è un agente, perché la conversazione non implica autonomia.

Automazione tradizionale (RPA o robotic process automation)

L'RPA esegue script fissi su interfacce strutturate. Sposta dati tra sistemi, riempie form, riconcilia tabelle. Replica esattamente quello che farebbe una persona seguendo una procedura scritta. UiPath che riconcilia transazioni tra ERP e CRM è il caso d'uso classico.

Il limite è altrettanto strutturale: l'RPA si rompe quando il processo o l'interfaccia cambia anche di poco. Non interpreta dati non strutturati, non gestisce eccezioni, non decide.

Pensare che un agente sia un RPA con un LLM dentro è molto limitante, perché l'agente vero non segue un binario, sceglie il binario.

AI agent

L'agente AI vero riceve un obiettivo, ragiona su come raggiungerlo, sceglie gli strumenti (API, modelli predittivi, modelli generativi), adatta il percorso alle eccezioni e decide quando ha finito o quando passare la palla a una persona.

La definizione canonica viene da Anthropic, azienda madre di Claude: “gli agenti sono sistemi in cui i modelli linguistici dirigono in modo dinamico i propri processi e l'uso degli strumenti, mantenendo il controllo su come portare a termine i compiti” (Anthropic, *Building effective agents*).

Tre elementi permettono di riconoscere un agente vero, indipendentemente dalle parole con cui lo si presenta:

1. decide il *come*, non si limita a eseguire il *cosa*;
2. gestisce le eccezioni invece di bloccarsi, anche solo riconoscendole e passandole all'umano in modo informato;
3. usa più strumenti in sequenza adattiva, non un singolo flusso lineare.

L'agente raccontato in apertura di questo documento, quello che ha preparato la riconfigurazione dell'ordine annuale del cliente di componentistica industriale, è esattamente questo.

Ha deciso il come (quattro fonti incrociate in autonomia: storico forniture, scorte, previsioni di domanda, contratti). Ha gestito l'eccezione (i punti fuori perimetro segnalati alla sala procurement, separati da quelli pre-autorizzati su cui ha agito direttamente). Ha usato più strumenti in sequenza adattiva (lettura mail, classificazione, retrieval da quattro sistemi diversi, generazione documento, redazione nota tecnica).

Tabella 1. I tre sistemi tecnologici.

Categoria	Cosa decide	Cosa NON fa	Esempio
Copilot / chatbot assistivo	Niente, suggerisce	Eseguire azioni in autonomia	ChatGPT (chat)
RPA	Niente, esegue script	Gestire eccezioni o dati non strutturati	UiPath che riconcilia ERP e CRM
AI agent	Come raggiungere un obiettivo	Decisioni fuori dal perimetro che gli è permesso	Agente customer service end-to-end con escalation contestualizzata

Spesso non è facile distinguere questi ultimi due scenari, motivo con cui si spiega l'alta percentuale di aziende convinta di aver implementato un agente quando ha solo attivato un workflow AI.

Nella fase ancora iniziale e sperimentale in cui ci troviamo, i due ambiti sono in effetti poco differenziabili e a volte quasi sovrapposti, specialmente quando il workflow AI comprende LLM + RAG + orchestrazione.

La differenza sostanziale da tenere a mente, anche nel leggere gli esempi del prossimo capitolo, è che si inizia a distinguere un processo agentico quando ci sono almeno alcuni di questi elementi:

- autonomia contestuale,
- selezione dinamica di strumenti/fonti,
- reasoning multi-step,
- goal-oriented execution.

2.2 Quando un'azienda diventa agentica

Fin qui, questo capitolo ha parlato di sistemi tecnologici: cosa fa una macchina.

Ma l'*Agentic enterprise* non è un sistema, è una **persona giuridica con certe caratteristiche organizzative**. Non si compra in licenza, si raggiunge per scelte deliberate e cumulative.

Avere un agente in produzione non equivale a essere un'agentic enterprise.

Cinque elementi distinguono un'azienda *agentica* da un'azienda *con agenti*:

1. Multi-agent orchestrati. Gli agenti parlano tra loro e si coordinano, non vivono in silos disconnessi. Un'azienda con tre agenti customer service che non si parlano e con un agente di compliance separato non è agentica, è una collezione di automatismi.

Il *2026 Connectivity Benchmark Report* di Salesforce, condotto su 1.050 IT leader enterprise, documenta che il 50% degli agent attualmente in produzione opera in silos isolati anziché come parte di un sistema multi-agent, generando workflow disconnessi, automazioni ridondanti e rischio di shadow AI (Salesforce, *2026 Connectivity Benchmark Report*).

50%
of AI Agents operate in silos rather than a part of a multi agent system

27%
of applications are connected together

Fonte: Salesforce, 2026 Connectivity Benchmark Report, febbraio2026

2. Governance esplicita con bounded autonomy. Stabilisce cosa decide l'agente, entro quale perimetro può agire in autonomia (la *bounded autonomy* della scena di apertura), quando deve passare la palla all'umano e come si traccia ogni decisione. L'essere umano non viene sostituito, ma abilitato al governo della macchina e all'intervento diretto dove davvero importante. La governance è il telaio progettuale dell'intera architettura. Senza governance esplicita e bounded autonomy, l'autonomia degli agenti rappresenta un rischio operativo e legale.

L'Osservatorio AI del Politecnico di Milano lo conferma esplicitamente: “fino al raggiungimento della piena maturità tecnologica [...] la strategia più efficace resterà un approccio human-in-the-loop dove l'esecuzione operativa viene delegata all'agente, ma la governance strategica rimane in capo all'essere umano” (Osservatorio AI PoliMi 2025, pag. 35-36).

3. Workflow ridisegnati. I processi sono ripensati per l'agente, non il contrario: l'agente non viene semplicemente “incollato” sopra un vecchio processo. Una catena di workflow del 2018 con un agente messo a monte non è agentic enterprise ma “automazione cosmetica”. Il ridisegno è la parte forse più importante, e più complessa, del lavoro.

4. Persone presidianti integrate. Servono figure interne stabili: sponsor di alto livello con potere decisionale, knowledge manager dedicati alla cura della knowledge base, project manager con visione operativa fra agente e processi. Senza queste figure, mancano i presidi necessari a governare gli agenti.

5. Visione di lungo termine dichiarata. Una roadmap a 18-24 mesi che includa il fine tuning post go-live come parte integrante del progetto, non come anomalia. Le aziende che trattano il primo go-live come traguardo finale tendono a fermarsi al primo agente. Le aziende che lo trattano come prima tappa di un viaggio organizzativo, si dirigono verso l'Agentic Enterprise.

Gartner prevede che il 40% delle enterprise application avrà AI agent integrati entro fine 2026, contro meno del 5% nel 2025 (Hype Cycle for Agentic AI 2026). Aver integrato AI agent nelle applicazioni e essere un'agentic enterprise sono però due cose diverse. La prima è una condizione tecnologica, cresce per integrazioni verticali nelle piattaforme. La seconda è una condizione organizzativa, che cresce per scelte deliberate e tempi più lunghi. La maggior parte delle aziende sarà nella prima ma non nella seconda nei prossimi due anni, e l'agentic enterprise resta un traguardo di lungo termine verso cui lavorare per step.

Tabella 2. Azienda con un agente vs agentic enterprise.

Dimensione	Azienda con AI agent	Agentic enterprise
Numero di agenti	Un agente per caso d'uso	Multi-agent orchestrato
Governance	Implicita, ad hoc	Esplicita, con audit trail su ogni interazione
Workflow	Vecchi processi + agente	Processi ridisegnati per l'agente
Persone interne	Sponsor del progetto	Sponsor + KB manager + PM dedicati
Visione temporale	Caso d'uso	Roadmap 18-24 mesi dichiarata

Tre aziende italiane stanno facendo esattamente questo. Le pagine che seguono raccontano cosa hanno trovato sulla strada.

GUNPOWDER

03

CAPITOLO 3

3 Gradini che bloccano l’azienda

3.0 Gli step della scala agentica

Il viaggio verso un'agentic enterprise passa attraverso vari gradini sequenziali.

Per tutto ciò che abbiamo visto finora, saltare gli step o affrettarsi a scapito del metodo è rischioso: lo si paga con ritardi, ripensamenti, cicli di riprogettazione o, nel peggiore dei casi, go-live che non risolvono nulla pur avendo consumato risorse, budget e aspettative.

Chi è fermo al primo gradino, o non l'ha ancora affronta- to, vede solo l'inizio del percorso: è quello più alto, su cui si fatica maggiormente a salire perché richiede un cambio di mentalità e approccio.

Si tratta di decidere come governare il processo e dove allocare i dati e i modelli proprietari in base alle proprie necessità, vincoli normativi e tecnologici.

Chi ha iniziato a muoversi si accorge che dietro quel primo gradino ce n'è un secondo. La strategia di deploy- ment, il sequencing dei workflow, la resistenza alle pressioni per accelerare a scapito della sostenibilità del sistema. In questa fase il rischio principale è partire male, con fretta e senza visione di lungo periodo.

Chi percorre la scala e si avvicina al go-live scopre che dietro quel secondo gradino ce n'è un terzo, da non sottovalutare. La differenza tra un progetto di laboratorio e un agente operativo nel mondo reale: è dove si valuta la sua capacità di gestire eccezioni, di integrarsi con sistemi legacy, di operare in modo autonomo ma sicuro, nel rispetto dei vincoli di governance e di sicurezza definiti.

È la prova della realtà: cosa succede quando l'agente esce dalla sandbox e incontra clienti veri, processi veri, eccezioni che non erano testabili.

Ogni gradino occlude la vista del successivo. Chi è anco- ra fuori vede solo il primo, e spesso lo trasforma in un alibi per non partire. Chi ha iniziato a salire scopre, dal pianerottolo, che dietro c'è altro. E che il modo per supe- rarlo si capisce solo per iterazioni, tentativi ed errori.

3.1 Primo gradino: dove tenere i dati e i modelli

Il primo gradino arriva prima ancora di pensare al primo agente. È la domanda che si pongono molti C-level italiani, specie nelle aziende regolate, della pubblica amministrazione, di sanità, financial services, energy, insomma di tutte quelle organizzazioni con dati sensibili, quando guardano l'AI generativa e si chiedono cosa farne.

“Dove tengo i miei dati e i miei modelli?”

Le opzioni architetturali oggi sono in sostanza tre.

- **Cloud pubblico:** infrastruttura condivisa e multi-tenant, gestita da un provider terzo. È la categoria degli hyperscaler extra-UE (AWS, Microsoft Azure, Google Cloud) e dei provider europei (OVHcloud, Aruba, Open Telekom Cloud, IONOS). Si paga a consumo, si scala in fretta, l'hardware lo gestisce il fornitore.
- **Cloud privato:** infrastruttura dedicata a una singola organizzazione, isolata dal resto, che può vivere in una regione del provider con clausole specifiche, o nel data center del cliente. Costa di più, è meno elastico, ma garantisce un livello di isolamento che il public cloud non offre.
- **On-premise:** server fisici dentro il perimetro aziendale, sotto controllo diretto dell'IT interna. Massima sovranità, minore elasticità.

Per le organizzazioni che operano sotto AI Act, GDPR, normativa di settore, la scelta non è scontata. Il cloud pubblico, anche europeo, funziona per chi non ha quei vincoli, ma alcuni dati semplicemente non possono uscire dal perimetro aziendale, e alcuni modelli non possono essere chiamati attraverso API gestite da fornitori extra- UE senza una catena di garanzie precise.

Il primo gradino, in pratica, deve trasformare un vincolo regolatorio in una scelta di posizionamento.

Sovranità del dato come scelta, non come compromesso

La risposta di architettura che oggi funziona meglio per i settori regolati è una combinazione di tre elementi: deployment on-premise, modelli LLM open-source, retrieval RAG (Retrieval-Augmented Generation) su documentazione propria. Questi tre elementi consentono di mantenere il controllo completo sull'infrastruttura e sui dati, senza rinunciare alle capacità di un agente moderno.

Il vantaggio collaterale di questa scelta è questo: chi sceglie sovranità del dato costruisce di necessità anche una **governance più solida**, perché il vincolo regolatorio costringe a definire in anticipo chi traccia cosa, chi risponde di cosa, dove l'agente può agire in autonomia e dove deve passare la palla all'umano, esattamente come previsto dalla *bounded autonomy*. Spesso nel cloud "default" la governance arriva dopo l'integrazione, mentre qui viene per forza prima.

Salesforce, nel *2026 Connectivity Benchmark Report*, cita un dato che chiarisce la portata del problema oltre la sola PA.

Il 42% dei leader IT enterprise indica **risk management, compliance e legal come prima barriera all'agentic transformation**. Il 96% delle organizzazioni dichiara di incontrare barriere significative nell'usare i propri dati per casi d'uso AI (Salesforce, *2026 Connectivity Benchmark Report*).

La sovranità del dato non è una preoccupazione che riguarda solo ambienti iper-regolati come la PA, ma è una barriera trasversale che impatta tutto il mercato enterprise.

CASO — REGIONE ABRUZZO

Il caso Regione Abruzzo: RA-Copilot dentro lo sportello regionale

Regione Abruzzo è una delle tante pubbliche amministrazioni italiane impegnate in un percorso di digitalizzazione dei servizi e modernizzazione dei processi amministrativi.

Per rispondere alle stringenti necessità della PA, Giano, la piattaforma agentica di Gunpowder, è stata integrata all'interno di **RASportello**, il portale regionale per la gestione delle pratiche e delle istanze presentate dai cittadini.

In questo modo, l'architettura scelta è quella di sovranità totale. Giano è stato installato **on-premise** sull'infrastruttura della Regione. I modelli LLM sono sia **open-source che commerciali** (la piattaforma supporta GPT, Gemini, LLaMA, Mistral, Gemma, Phi, installabili localmente, scelti con un approccio ibrido a seconda dei casi di utiliz- zo) e il retrieval semantico avviene tramite RAG sulle knowledge base normative regionali.

Cosa fa concretamente Giano, diventato RA- Copilot, dentro RASportello?

Il valore dell'agente AI emerge soprattutto nella riduzione del carico cognitivo associato alla ricerca e all'analisi normativa e documentale, che è uno dei principali colli di bottiglia nei processi istruttori della PA.

Prendiamo come esempio reale l'istanza di taglio alberi, ovvero la richiesta di autorizzazione amministrativa che un cittadino presenta alla Regione per tagliare alberi su un'area sottoposta a vincoli di verde pubblico o paesaggistici, una fra le decine di tipologie normativamente eterogenee che RASportello gestisce.

Quando un cittadino presenta la pratica, l'agente: analiz- za autonomamente i documenti allegati, identifica il dominio amministrativo della pratica, in questo caso la gestione del verde pubblico, seleziona la base normativa pertinente fra le diverse che la Regione gestisce, esegue retrieval semantico sulla documentazione interna, e produce un'analisi preliminare della pratica.

L'output che arriva sulla scrivania del valutatore regiona- le include così un riassunto della pratica, con criticità e vizi di forma rilevati automaticamente, verifiche istruttorie suggerite, riferimenti normativi precisi, chat AI contestuale specializzata sul dominio normativo per approfondimenti puntuali durante l'istruttoria.

RA-Copilot non è esposto ai cittadini, non è quindi un chatbot messo davanti allo sportello. Vive dentro il portale operativo dei dipendenti regionali e supporta il loro lavoro di pre-istruttoria.

La validazione finale della pratica, l'approvazione o il rigetto dell'istanza, restano in capo all'operatore umano, applicando la bounded autonomy: l'agente opera auto- nomamente nella fase di pre-istruttoria, ma la decisione amministrativa resta integralmente sotto il controllo umano del funzionario, che decide e firma.

Perché questo è un caso agentico e non un workflow AI?

In questo scenario, un workflow AI tradizionale determinerebbe il dominio amministrativo e la normativa applicabile tramite regole statiche, classificazioni predefinite o mapping configurati a monte.

Nel caso di RA-Copilot, invece, è l'agente a determinare dinamicamente quale corpus normativo interrogare sulla base del contenuto semantico della pratica, dei documenti allegati e del contesto amministrativo emergente.

L'agente non si limita dunque a generare testo o sintetizzare documenti: costruisce autonomamente una catena operativa composta da classificazione contestuale, selezione delle fonti normative, retrieval semantico, reaso- ning istruttorio e generazione dell'output operativo.

L'orchestrazione non è quindi rigidamente deterministica, ma adattiva e context-driven: è questo il passaggio da AI workflow automation ad agentic AI. Inoltre l'agente opera seguendo una logica goal-oriented, nella quale l'obiettivo non è generare una risposta conversazionale, ma produrre un supporto istruttorio coerente con il dominio amministrativo rilevato.

“Il valore dell'AI generativa nella PA dipende dalla qualità documentale, dalle basi normative strutturate, dalla governance informativa e dall'infrastruttura”, sintetizza Davide Iacobelli, Head of BI & AI Competence Center di Gunpowder. Quattro elementi che sono i prerequisiti operativi dell'agentic enterprise, come già visto nel capitolo precedente.

Il caso è oggi a livello pilot, su un insieme limitato di tipologie pratiche (oltre al taglio alberi, anche le verifiche di conformità per i cantieri edili e alcuni domini affini di gestione amministrativa). I volumi quantitativi e i KPI di efficienza non sono ancora pubblici. La copertura è destinata a estendersi nei prossimi mesi, per tipologia pratica e per ufficio coinvolto.

CASO — REGIONE MARCHE

Lo stesso schema, replicato: Regione Marche

Il caso Regione Abruzzo non è isolato nella PA italiana. Dentro la sperimentazione nazionale Reg4AI, la Regione Marche si è affidata a Gunpowder per sviluppare una piattaforma tecnologica, con architettura analoga a quanto visto sopra, su cui verranno attivati una pluralità di agenti, per la verifica documentale dei bandi pubblici e altre attività.

Stesso approccio operativo: human-in-the-loop pulito (l'agente segnala anomalie al funzionario, non procede in autonomia), comprensione semantica del contenuto documentale, prerequisito di knowledge base ripulita e governance interna in revisione. La stima attesa al rilascio completo è di una **riduzione dell'80% del tempo dedicato al controllo documentale di routine**.

La sovranità del dato applicata alla PA italiana non è quindi scelta virtuosa di una singola regione, ma un mo- vimento che si sta consolidando dentro la sperimentazione nazionale.
La governance che è necessario costruire per ragioni regolatorie si rivela esattamente quella che servirà al secondo gradino, dove il problema cambia natura ma non sostanza: come distribuire agenti in modo sicuro e controllato, con risk management, audit, human-in-the-loop, e scalabilità operativa.

3.2 Secondo gradino: gradualità contro big bang

Decisa l'architettura, viene il momento di costruire. È qui che molte aziende, soprattutto le grandi enterprise con stack tecnologici stratificati negli anni, scivolano.

“Da dove comincio, se sono un colosso con SAP legacy con processi multi-sistema?”

La risposta “dall'agente” è sbagliata.

Un processo agentico, per funzionare, arriva alla secon- da o alla terza tappa di un percorso più lungo. Saltare la prima significa aver “messo l'AI nei processi”, senza aver mai ridisegnato il terreno su cui l'AI deve operare.

Tre tappe sequenziali

Per una grande enterprise o per una PMI, il viaggio agentico ha tre tappe ben distinte.

Prima tappa: integrazione e orchestrazione dei sistemi che già ci sono. Rendere parlanti SAP, mainfra- me, ERP custom, CRM, sistemi documentali e di work-flow. È un lavoro di plumbing, di integrazione: permette di far dialogare le “tubature” fra i sistemi esistenti. Non certo glamour, ma decisivo per quello che viene dopo. Senza una catena di sistemi che si parlano, infatti, l'agente conversazionale non ha terreno utile su cui muoversi.

Seconda tappa: agente conversazionale. Introdurre comprensione semantica e capacità decisionale dentro un processo aziendale ormai orchestrato. Un singolo agente che fa una cosa bene, su un perimetro definito, con i sistemi che gli stanno intorno già allineati.

Terza tappa: multi-agent e algoritmi adattivi. Più agenti specializzati che si coordinano, orchestrati da una logica di livello superiore. È la frontiera operativa dell'agentic enterprise, dove gli aspetti di ridisegno orga- nizzativo e di governance diventano centrali.

L'ordine non è negoziabile. Saltare la prima tappa significa mettere un agente intelligente sopra dati frammentati: la sua intelligenza viene neutralizzata dalla qualità dell'input. Saltare la seconda significa costruire un'orchestrazione fra agenti che non sanno ancora gestire i propri singoli casi, il che amplifica gli errori invece di ridurli.

CASO — AXPO / LEVI

Il caso AXPO di LEVI in tre tempi

AXPO è un grande operatore del settore Energy & Utilities, con processi già strutturati su SAP IS-U in conformità alle normative ARERA. Azienda matura, con una infrastruttura solida e ben definita, ma con una necessità specifica: chiudere il “buco nero comunicativo” del recupero crediti verso l'esterno.

LEVI è il prodotto che Gunpowder ha sviluppato in risposta, per il credit management Salesforce-native: configurabile, flessibile, scalabile, low-code. Quello che AXPO ha adottato è un prodotto pronto all'uso che si appoggia sopra l'ecosistema Salesforce e si integra con i sistemi SAP del cliente. Il processo si sviluppa in tre tempi.

Ieri: il “buco nero” del recupero crediti verso l'esterno

Il recupero crediti di un grande operatore energy passa tipicamente attraverso attori esterni: studi legali, agenzie di riscossione, collector specializzati. Questa gestione, all'interno di AXPO, seguiva un percorso strutturato e tracciato dentro SAP. Ma nel momento in cui le pratiche venivano affidate all'esterno, la tracciabilità si interrompeva. Le informazioni uscivano dal perimetro SAP e si frammentavano in email, file Excel e messaggi.

Gli addetti interni AXPO erano così ridotti a fare i passacarte, impegnati nell'invio manuale di aggiornamenti pratiche verso i collector esterni. I collector erano a loro volta costretti a chiamare AXPO per ogni informazione che non passava dai canali ufficiali. I tempi di gestione erano lunghi, la qualità del dato variabile, e non c'era alcuna visibilità sincrona sullo stato della pratica.

Oggi: l'orchestrazione che ha chiuso l'ultimo miglio

LEVI opera oggi come interfaccia intelligente fra i sistemi core di AXPO (SAP ERP, SAP IS-U, PITECO per la gestione incassi, sistemi documentali) e i partner esterni. Tecnicamente, è un layer applicativo costruito su Salesforce Communities, che espone in modo strutturato e GDPR-compliant i dati del credit management ai collector autorizzati.

Cosa cambia per gli attori esterni? Uno studio legale che gestisce per conto di AXPO una pratica di recupero non telefona più per chiedere lo stato. Accede al portale LEVI, visualizza i dati del cliente assegnato, gestisce l'avanzamento della riscossione interagendo direttamente con il workflow, e apre case strutturati dentro il sistema invece di mandare email.

Cosa cambia per AXPO internamente? Il personale interno è uscito dal ruolo di passacarte ed è rientrato in attività professionali più elevate. Il repository SharePoint dedicato è stato spento, perché reso obsoleto dalla nuova interfaccia. I tempi di latenza per i collector si sono azzerati.

La differenza fra LEVI e un RPA tradizionale sta nell'ampiezza dell'integrazione e nella flessibilità low-code: LEVI non gestisce script fissi, gestisce un workflow che il cliente può riconfigurare. Ma il cuore decisionale è ancora del processo, non di un LLM. Tornando al fra- mework del capitolo 2, questo è ancora il piano dell'auto- mazione intelligente, non dell'agente vero.

Domani: l'interfaccia conversazionale e gli algoritmi adattivi

La roadmap LEVI di prossima produzione introduce due elementi che aggiungono un altro strato alla struttura. Il primo è l'interfaccia conversazionale: gli studi legali potranno interrogare LEVI a voce o via chat per ottenere informazioni sui vari stadi del recupero crediti, senza navigare il front-end. Il secondo sono algoritmi adattivi che faranno evolvere automaticamente la “gravità” del sollecito in base al comportamento del debitore, traducendo decisioni che oggi richiedono valutazione umana in suggerimenti puntuali.

L'interfaccia conversazionale è una capability di assistenza sopra dati orchestrati. Gli algoritmi adattivi sono AI predittiva che genera suggerimenti. Non ancora un agente che decide e agisce in relativa autonomia. Ciascuno dei due, però, aggiunge un'infrastruttura che prima non c'era: la prima introduce uno strato di comprensione semantica delle richieste, la seconda un cana- le di lettura del comportamento del debitore.

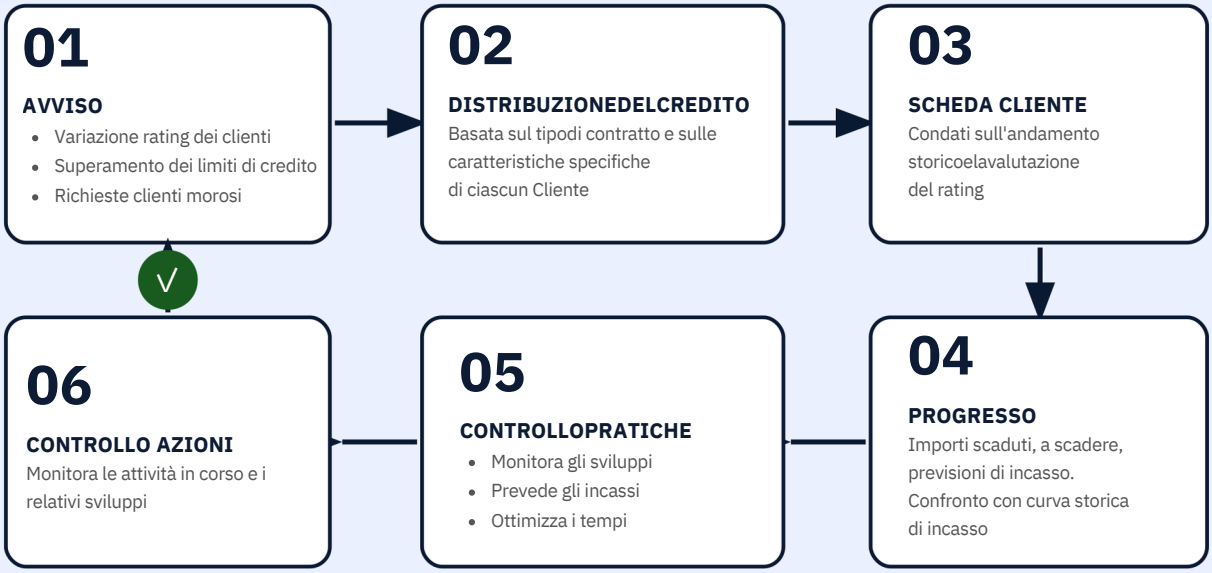
Da lì in avanti, si potranno implementare funzionalità sempre più evolute e autonome, perché il terreno per farlo sarà stato costruito una tappa alla volta. Ogni passaggio costringe a creare un'infrastruttura che altrimenti non esisterebbe, e ciascuna infrastruttura abilita la successiva.

L'agentic enterprise non è un traguardo a cui si arriva con un salto: è la somma di scelte tecniche e organizza-

tive che si chiudono in sequenza, e ciascuna di queste scelte è il prerequisito di quella che viene dopo.

Il secondo step è quindi una moltitudine di gradini più piccoli. Ciascuna organizzazione deve capire quanti e quali siano in base al proprio progetto e obiettivo finale di automazione, sapendo che le prime soluzioni non dovranno essere agentiche, ma saranno il prerequisito che rende possibile per un sistema agentico operare in autonomia, al momento giusto.

Mappa diprocesso
Sistema di gestione del credito LEVI



Fonte: Gunpowder.

3.3 Terzo gradino: dal pilot alla realtà

Quando l'agente esce dalla sandbox e incontra clienti veri, si apre un altro tipo di scenario: quello che si scontra con la realtà in continuo divenire dell'AI e delle soluzioni proposte.

Le piattaforme agentiche enterprise oggi sono in maturazione costante, e questo significa instabilità early-stage che non è prevedibile e necessità di adattamenti continui.

Gli SDK degli AI agent rilasciano nuove release ogni pochi mesi. Anthropic e OpenAI aggiornano i modelli sot- tostanti con cadenze ravvicinate. Gli stack enterprise (Agentforce, Copilot Studio, ServiceNow AI Agents, ecc.) sono in continua evoluzione.

Fa parte delle regole del gioco: non si può attendere che la tecnologia sia perfettamente stabile prima di partire, perché significherebbe lasciarsi superare e creare un gap incolmabile.

Bisogna quindi considerare la fase di release come una “sandbox aperta”, in cui proprio gli attriti e le difficoltà sono ciò che permette di migliorare il risultato: i bug platform-level che emergono solo a contatto con il traffico vero indicano dove intervenire, i comportamenti dell'agente che divergono dai test di laboratorio servono a tracciare vincoli e confini, le integrazioni con i sistemi legacy vanno affinate e customizzate.

CASO — UBROKER / UBI

Il caso uBroker: come arrivare a un bot che funziona davvero

uBroker è un fornitore italiano di energia elettrica e gas attivo dal 2015, nato a Torino e oggi presente su tutto il territorio nazionale. Il modello commerciale innovativo è basato sul programma di fidelizzazione per passaparola dai clienti soddisfatti: coloro che portano nuovi contratti possono arrivare ad azzerare le proprie bollette. L'azienda ha ricevuto riconoscimenti per crescita, innovazione e pratiche ESG, ed è culturalmente orientata all'adozione precoce di nuove tecnologie.

In virtù del suo posizionamento innovativo, uBroker voleva portare l'AI nel settore energy italiano, con priorità sulla customer experience prima ancora che sull'efficien- za economica. Da questo desiderio e dalla collaborazio- ne con Gunpowder è nato Ubi, l'agente AI conversazionale di uBroker.

Architettura e principio “Human-First”

Ubi è un AI agent conversazionale costruito su Salesfor- ce Agentforce, con Atlas Reasoning Engine come moto- re decisionale e un Trust Layer che include data ma- sking, toxicity detection, zero data retention e prompt defense. Il cuore del funzionamento di Ubi è una know- ledge base completa e curata, con oltre 500 FAQ conti- nuamente aggiornate da una persona dedicata, un ruolo definito appunto Knowledge Manager.

Grazie a questo database, l'agente ricava le risposte alle domande degli utenti, gestisce le conversazioni in linguaggio naturale e si integra con gli altri sistemi azienda- li per fornire un servizio completo (Salesforce Service Cloud come hub centrale e il CRM per l'identificazione del cliente durante la conversazione). I canali di eserci- zio sono multipli: WhatsApp, chat sul sito aziendale, chat nell'area clienti dell'app, con voicebot in via di integrazione come seconda fase.

Dentro la cornice della *bounded autonomy*, uBroker ha scelto un approccio “Human-First”: Ubi dichiara subito la propria identità e offre immediatamente all'utente la scelta di un operatore umano. Questo approccio elimina ogni possibile frustrazione, posizionando l'AI come un supporto e mai come un ostacolo.

Il primo mese in produzione

Il go-live di Ubi è del 15 aprile 2025. Come ogni messa in produzione di un sistema complesso, anche quello di Ubi ha incontrato la realtà fuori dai test al primo contatto con il traffico vero, evidenziando problemi che non potevano essere previsti in laboratorio.

Con un agente AI questo è ancora più fisiologico che con un software tradizionale: **l'agente decide in auto- nomia, le risposte non sono predefinite, e certi com- portamenti emergono solo davanti a casi reali e a un mix imprevedibile di richieste.**

Alcune imperfezioni a livello di piattaforma avevano impatto sull'esperienza dell'utente finale: comportamenti legati a tipi di input non standard, alla reattività percepita del sistema, al modo in cui l'agente interpretava certe categorie di richieste. Le problematiche sono state segnalate tempestivamente a Salesforce, che si è impe- gnata a risolverle, ma i tempi tecnici hanno messo sotto pressione uBroker sul progetto Ubi.

In questa fase Gunpowder, in quanto partner tecnologico di uBroker, si è posizionata a presidio diretto del proget- to, canalizzando l'interlocuzione tecnica con Salesforce. Il lavoro ha portato a stabilire con uBroker un perimetro operativo condiviso per gestire la fase di attesa, mantenendo Ubi operativo sui canali in produzione. Quando è arrivata la release Agentforce che ha sistemato i comportamenti emersi, il progetto è uscito dalla fase critica senza interruzioni di servizio ed è potuto diventare ciò che è oggi: un sistema di IA conversazionale in continua evoluzione, capace di migliorare costantemente in funzione delle reali esigenze degli utenti.

Cosa ha prodotto la stabilizzazione

Dopo la stabilizzazione, i numeri di Ubi misurati nel 2026 raccontano un agente che porta ottimi risultati. Il **deflection rate in orario lavorativo è del 25%**: una richiesta su quattro che arriva sui canali digitali si chiude senza coinvolgere un operatore umano. La copertura è estesa a H24, sette giorni su sette, dove prima esisteva solo nelle ore lavorative. La knowledge base continua a cre- scere, arricchendosi in base ai nuovi scenari di utilizzo reale.

Gli operatori del customer service sono stati liberati dalle richieste ripetitive e si dedicano oggi a casistiche complesse. I nuovi operatori usano Ubi come strumento di formazione interna, accelerando la propria curva di apprendimento. La KB costruita per l'agente ha avuto un effetto di standardizzazione delle informazioni disponibili per tutto il customer service.

Sull'onda di questi risultati, uBroker ha portato Ubi a Utility Day 2025 candidandolo al premio *Best AI Applica- tion and Automation Project*, consolidando il posiziona- mento dell'azienda come early adopter del settore ener- gy.

La roadmap di Ubi prevede una fase 2 con azioni dispo- sitive (invio bollette su richiesta autenticata, lettura OCR di contabili di pagamento, raccolta autoletture) e una fase 3 con voicebot integrato all'IVR telefonico. Oggi uBroker sta ragionando con Gunpowder su nuovi agenti, dopo aver già integrato un "clone" di Ubi in un'altra compagnia del gruppo.

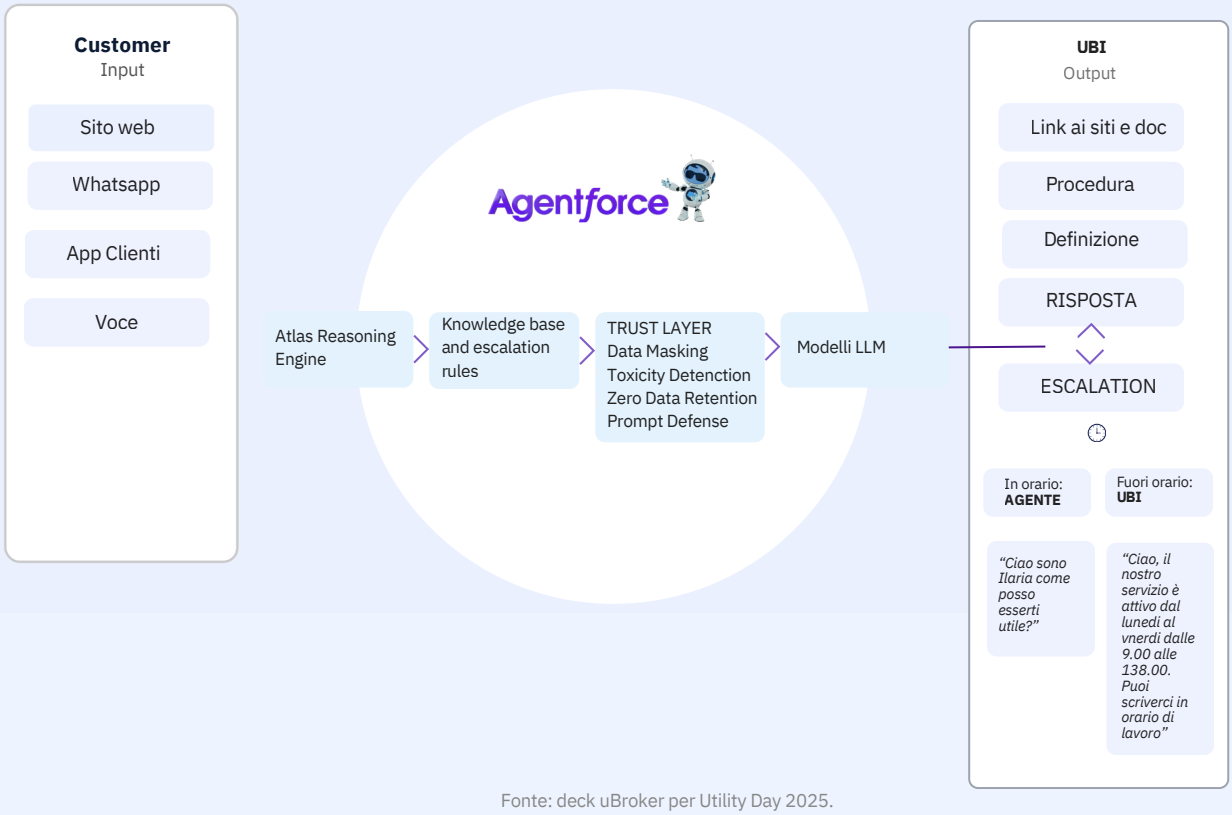
Le evoluzioni agentiche del customer service

L'uso di agenti nel customer service è già ora una delle applicazioni più mature dell'AI aziendale, ma il salto di qualità è rappresentato da un agente vocale che com- prende l'intento dell'utente, consulta la knowledge base, decide come rispondere, eventualmente apre un ticket, e fa handover contestualizzato a un operatore umano quando serve.

Un'azienda italiana del settore mobilità e telepedaggio sta testando, in fase finale di POC, un agente vocale costruito da Gunpowder su Agentforce Voice. Il feedback emerso in demo è di grande "effetto wow" sulla natura- lezza dell'interazione, con deflection attesa al rilascio del 10-20% sulle richieste ricorrenti, copertura H24 sette giorni su sette, conversazioni registrate e analizzabili a fini di miglioramento continuo.

Un'ulteriore evoluzione è la Sentiment & Conversation Intelligence: l'analisi delle conversazioni cliente in real- time, per intercettare escalation emotive o opportunità di risoluzione immediata, con batch sulle registrazioni stori- che, per identificare pattern, casi d'uso da automatizza- re, qualità del servizio per operatore. La Conversation Intelligence diventa il sistema nervoso del customer service agentico: l'agente migliora grazie alle conversa- zioni che gestisce, e gli operatori umani sono allertati dove l'intervento serve davvero.

Come funziona UBI—Architettura tecnica



Fonte: deck uBroker per Utility Day 2025.

GUNPOWDER

04

CAPITOLO 4

La matrice della scelta architetturale

4.0 I due assi della scelta architetturale

Il primo passo per avvicinarsi alla scala che porta all'Agentic Enterprise è, come accennato, la scelta architetturale che sta alla base del sistema. Stack tecnico, perimetro di sicurezza, tipo di partner, persino cultura organizzativa, tutto discende da lì.

Questa scelta dipenderà ovviamente in gran parte dall'architettura corrente dell'organizzazione: che tipo di CRM, ERP, gestionali vari già utilizza, specialmente nel caso delle grandi aziende consolidate; e quale livello di autonomia e sicurezza dei dati ha bisogno di mantenere, in base a normative, settore, etc.

Per descrivere questa scelta e le sue diverse opzioni possiamo quindi utilizzare due assi indipendenti:

- **Sovranità sui dati:** dove vivono i dati e chi li controlla. Alta sovranità = dati on-premise o in cloud sovrano; bassa = dati nel cloud gestito da un vendor o da terzi.
- **Ecosistema:** quanto ci si appoggia su un grande vendor enterprise consolidato. Alto = dentro Salesforce, Microsoft, ServiceNow, ecc.; basso = piattaforma indipendente o stack multi-vendor.

I due assi sono indipendenti, e combinati danno quattro quadranti. Gli elementi che compongono i due assi indipendenti emergono da diverse analisi di settore, tra cui quella di Kai Waehner sull'Enterprise Agentic AI Landscape, che pone trust nel vendor e lock-in di ecosistema fra le due dimensioni decisionali principali in ambito AI. Vediamo quali sono le quattro architetture che ne derivano.

Matrice della scelta architetturale

	Basso ecosistema	Alto ecosistema
Alta sovranità	**Sovranità indipendente** **Piattaforma propria, dati in casa. Giano on-premise è l'esempio tipico.**	**Ecosistema sovrano** **Grande vendor portato in casa o in cloud sovrano dedicato.**
Bassa sovranità	**Architettura composita** **Soluzione multi-vendor, stack assemblato con API e MCP.**	**Ecosistema gestito** **L'AI vive dentro il cloud del vendor (Salesforce, Microsoft, ServiceNow).**

4.1 Ecosistema gestito: l'AI vive dentro il cloud del vendor

Bassa sovranità · Alto Ecosistema

Probabilmente è il quadrante più popolato del mercato enterprise oggi. Gli agenti si costruiscono dentro una piattaforma enterprise che il business già usa, ereditano dalla piattaforma host modello dei dati, permission, trust layer, audit trail e integrazioni native, e vivono nel cloud gestito dal vendor.

Gli esempi di mercato consistenti nel 2026 sono diversi, tra cui: Salesforce Agentforce, agenti dentro l'ecosistema Service Cloud, Sales Cloud, Data Cloud; Microsoft 365 Copilot Studio, integrato nella tenant di Azure AD, con sicurezza Entra e parlante con Teams, Outlook, SharePoint; ServiceNow AI, agenti disponibili dentro la piattaforma di service management, con accesso ai workflow CMDB e ITSM.

In tutti i principali casi, le capability agentiche sono native dell'applicazione che il business già usa, non applicazioni separate che si appoggiano all'ecosistema con API.

Vantaggi

- Implementazione rapida, con configurazione low-code o no-code. Per casi d'uso comuni (customer service, sales assistance, IT help desk) il time-to-prototype è abbastanza breve.
- Compliance e sicurezza ereditate. Il vendor ha già investito in certificazioni, audit, data residency. Le capability agentiche ereditano l'infrastruttura di fiducia.
- Adozione facile per chi è già nell'ecosistema. Gli operatori percepiscono gli agenti come funzioni in più dell'applicazione che usano da anni, e la curva di adozione è bassa.

Limiti

- Personalizzazione limitata ai ruoli e alle configurazioni che la piattaforma host espone. Per workflow oltre i casi d'uso standard del vendor, la configurazione (quando è possibile) necessita di competenze tecniche specialistiche.
- Dipendenza dall'ambiente vendor: roadmap, prezzi ed evoluzione delle feature dipendono dal vendor.
- Difficoltà a estendersi a sistemi fuori dall'ecosistema: integrazioni con sistemi gestionali diversi, mainframe legacy o sistemi documentali di terze parti esistono, ma non sono nativi.

Quando ha senso

- Aziende già fortemente integrate in un ecosistema vendor.
- Casi d'uso che vivono dentro quell'ecosistema.
- Priorità su rapidità di go-live e curva di adozione bassa.
- Dati che le certificazioni standard del vendor coprono già.

I confini di questo quadrante si stanno spostando rapidamente, trasformando le piattaforme da SaaS per umani in infrastruttura per agenti che il cliente compone, come vedremo nell'ultimo capitolo.

4.2 Sovranità indipendente: piattaforma propria, dati in casa

Alta sovranità · Basso ecosistema

In questo quadrante si posizionano le organizzazioni che hanno priorità massima sul controllo dei dati e sulla personalizzazione di dominio, e desiderano una piattaforma configurata sulle loro esigenze e un'infrastruttura interna. Gli agenti vivono su una piattaforma agentica indipendente dall'ecosistema applicativo del cliente, installata on-premise o in cloud sovrano, con modelli LLM open- source (o commerciali, se servono) e integrazione con i sistemi esistenti via API e MCP.

Un esempio che opera in questo quadrante è Giano, la piattaforma AI di Gunpowder che permette di integrare l'Intelligenza Artificiale nei propri sistemi esistenti, garantendo pieno controllo infrastrutturale, governance centralizzata e indipendenza dai provider.

Installata ad esempio sull'infrastruttura on-premise della Regione Abruzzo come RA-Copilot (il caso del capitolo 3.1), Giano utilizza modelli LLM scelti dal cliente e RAG sulle knowledge base normative regionali, mantenendo totale sovranità sui dati, sicurezza e controllo dei risultati, ma dando la possibilità all'utilizzatore di beneficiare dei migliori modelli LLM disponibili sul mercato.

Vantaggi

- Controllo completo su modelli e infrastruttura: i dati restano dentro il perimetro, i modelli sono selezionabili e sostituibili senza riprogettare il sistema.
- On-premise per i settori regolati, in linea con i vincoli AI Act, GDPR e classificazioni AgID.
- Integrazione universale, non legata a un singolo ecosistema. Una piattaforma sovrana può integrarsi con SAP, mainframe, ERP custom, sistemi documentali di terze parti.
- Personalizzazione avanzata sui domini proprietari, dove gli ecosistemi standard arrivano invece con modelli pre-configurati pensati per casi d'uso comuni.
- Governance strutturata dall'inizio del progetto, invece che aggiunta a posteriori.

Limiti

- Implementazione consulenziale, non plug-and-play. La piattaforma va costruita o adattata sulle esigenze cliente, senza blueprint pronti per ogni caso d'uso.
- Richiede un partner con competenze su più fronti:
- Time-to-value più lungo dell'ecosistema gestito, soprattutto se la knowledge base interna non è già strutturata.

Quando ha senso

- Organizzazioni con priorità su privacy e sovranità del dato: PA, sanità, financial services, energia, con dati sensibili.
- Patrimoni informativi distribuiti su sistemi eterogenei,
- Personalizzazione su necessità interne che vanno oltre i ruoli predefiniti di un vendor.

4.3 Architettura composita: soluzione multi-vendor

Bassa sovranità · Basso ecosistema

Il quadrante delle organizzazioni che non sono dentro un grande ecosistema vendor consolidato e non hanno vincoli regolatori stretti sui dati. Tipicamente costruiscono lo stack agentico assemblando vendor specializzati per funzione, sviluppando componenti custom su API di modelli, o combinando le due cose.

Le forme che il quadrante assume nel 2026: diverse piattaforme multi-vendor, ciascuna con le proprie funzionalità AI, che si parlano via API e MCP; piattaforme custom su API commodity (accesso diretto ai modelli di frontiera via API con sviluppo interno della logica agentica); piattafor- ma agentica indipendente in cloud non sovrano.

Vantaggi

- Strumento migliore per ciascuna funzione: ogni pezzo o piattaforma è scelto fra i migliori del segmento.
- Flessibilità di sostituzione: cambiare un vendor non implica riprogettare l'intero stack.
- Nessun lock-in di ecosistema: si è liberi dalle logiche di business di un singolo grande vendor.

Limiti

- Complessità di orchestrazione: serve qualcuno che faccia connettere correttamente fra loro vendor che non sono nati per integrarsi. La maturazione di MCP e A2A nel 2026 sta riducendo questo costo, ma non lo ha azzerato.
- Responsabilità di integrazione e governance a carico del cliente o del partner, non distribuita su un singolo vendor.
- Costo operativo distribuito su contratti, SLA e supporti tecnici di più vendor.

Quando ha senso

- Aziende mid-market non ancora entrate in un grande ecosistema enterprise.
- Esigenze funzionali specifiche, dove scegliere vendor specialistici produce vantaggio competitivo.
- Competenze interne tecniche forti, o un partner di integrazione esperto.

4.4 Ecosistema sovrano: il grande vendor portato in casa

Alta sovranità · Alto ecosistema

Il quadrante storicamente meno diffuso, ma in crescita nel 2026 grazie al movimento dei grandi vendor verso offering on-premise e cloud sovrano. L'azienda sceglie un grande vendor enterprise consolidato e mantiene contemporaneamente i dati e l'infrastruttura sotto controllo proprio, on-premise o in cloud sovrano dedicato.

Un esempio è Salesforce Hyperforce EU Operating Zone. Hyperforce è la nuova generazione dell'infrastruttura Salesforce, costruita come infrastructure as code per consentire deployment regionali, con dati che restano nella regione del cliente. Tuttavia si tratta di cloud regionale, non on-premise. Per la maggior parte dei vincoli GDPR e

AI Act è una risposta tecnicamente sufficiente, ma per il controllo totale si torna verso il quadrante della Sovranità indipendente.

Vantaggi

- Vantaggi del grande vendor ereditati (blueprint, integrazioni, supporto, certificazioni).
- Sovranità sui dati mantenuta, in linea con vincoli regolatori stretti.

Limiti

- Costo infrastrutturale molto alto: deployment on-premise o cloud sovrano dedicato costano di più del cloud condiviso del vendor.
- Versioni spesso limitate: alcune feature AI dei vendor sono disponibili prima nel cloud gestito e arrivano dopo nelle versioni sovrane.
- Complessità di aggiornamento: il deployment lo gestisce il cliente o il partner, non il vendor.

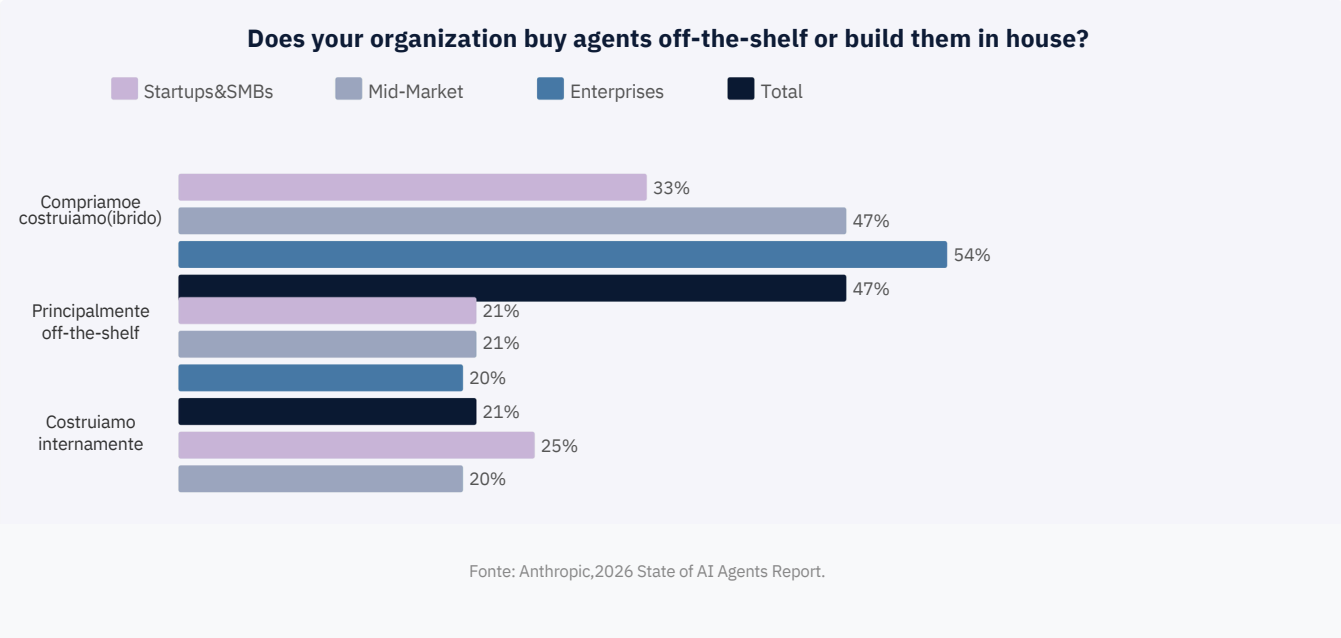
Quando ha senso

- Settori altamente regolati che vogliono restare nello stack di un grande vendor (aerospaziale, difesa, alcuni financial services, enti governativi).
- Grandi enterprise che hanno già investito nell'infrastruttura di un vendor e vogliono estenderne le capability AI senza spostare i dati.

4.5 A spasso tra i quadranti

Spesso le aziende mature collocano processi diversi in quadranti diversi, e disegnano lo stack agentico complessivo come composizione di queste scelte.

Secondo il *2026 State of AI Agents Report* di Anthropic, su 500+ leader tech enterprise, il 47% delle organizzazio- ni adotta un approccio ibrido, combinando soluzioni pre-configurate dell'ecosistema con componenti custom; solo il 21% sta interamente sul pre-built e il 20% costruisce tutto in casa (Anthropic, *2026 State of AI Agents Report*). La quasi maggioranza del mercato vive nel mezzo della matrice.



Fonte: Anthropic,2026 State of AI Agents Report.

Un esempio di coesistenza

Una multiutility italiana di grandi dimensioni potrebbe usare:

- Agentforce per il customer service multicanale (quadrante Ecosistema gestito: dati clienti standard, integrazione con Service Cloud già esistente, priorità alla rapidità).
- Una piattaforma agentica indipendente come Giano per la gestione documentale interna delle pratiche di compliance ARERA (quadrante Sovranità indipendente: dati sensibili, normativa stringente, knowledge base proprietaria su file server interni).
- Un tool specifico di marketing automation collegato via MCP al CRM (quadrante Architettura composita: best-in-class per la funzione marketing).

Stessa azienda, tre quadranti coesistenti, ciascun processo collocato dove i suoi vincoli e i suoi vantaggi pesano di più.

GUNPOWDER

05

CAPITOLO 5

Da dove partire e dove stiamo andando

5.0 Quanto dura il presente?

Tutto ciò che abbiamo visto nei capitoli precedenti non è statico. È un fotogramma di un mercato in movimento rapidissimo, e l'architettura, le competenze, la governance, le knowledge base che si stanno costruendo ora vanno pensate in funzione di dove andrà il mercato nei prossimi 18-24 mesi.

Bisogna agire ora così da non trovarsi fuori dai giochi tra due anni, ma avere ben chiara la velocità con cui tutto cambia: l'unica certezza che può guidare le nostre scelte, oggi, è la direzione in cui vogliamo andare.

Fra i movimenti in corso nel 2026 ce n'è uno che sta cambiando, sotto traccia, la natura stessa delle piattafor- me enterprise e rimescolando i quadranti della matrice vista nel capitolo precedente. Riguarda il loro riposiziona- mento da fornitori di applicazioni SaaS per umani a forni- tori di infrastrutture per agenti, componibili dal cliente. A 12-18 mesi ridisegnerà i termini della scelta architettura- le, ed è il prossimo livello a cui questo capitolo si apre.

5.1 Headless: il prossimo livello delle piattaforme enterprise

Le grandi piattaforme enterprise nate negli ultimi due decenni — Salesforce, Microsoft 365, ServiceNow, SAP — sono nate per essere consumate da utenti umani via interfaccia grafica, non da sistemi via API. Schermate, form, dashboard, workflow: il modello SaaS-per-umani è disegnato per essere gestito da chi siede davanti a un monitor.

Nel 2026 questo modello si sta affiancando a una secon- da postura del vendor: quella di fornire infrastruttura per agenti che il cliente compone. Ad aprile 2026, ad esem- pio, Salesforce ha annunciato Headless 360. Questa configurazione espone l'intera piattaforma Salesforce come API, MCP tool e CLI command.

Oltre 60 MCP tools e 30 coding skills preconfigurate per- mettono ai coding agent di terze parti (Claude Code, Cursor, Codex, Windsurf) di avere accesso diretto e live a dati, workflow e business logic di Salesforce, e di com- porre esperienze native su Slack, Voice, WhatsApp.

Non è una feature in più che si aggiunge alle funzionalità esistenti: questa mossa riposiziona Salesforce come un'infrastruttura per agenti, invece che per umani.

Cosa significa Headless in concreto

Significa che dati, workflow, regole di business e algoritmi della piattaforma diventano accessibili via API a qualun- que interfaccia digitale: portali custom, app mobile, siti e-commerce, chatbot e agenti AI, altri sistemi aziendali (ERP, gestionali legacy, sistemi documentali), applicazio- ni verticali costruite fuori dalla piattaforma, interfacce utente completamente rinnovate e personalizzate.

Salesforce resta il motore applicativo con i suoi dati, algoritmi e processi. Ma come questi vengono fruiti, e da chi, non è più limitato alle interfacce proprietarie del vendor. Il riposizionamento non è isolato. Microsoft con Copilot Studio + Graph apre dati e workflow di Microsoft 365 a sviluppo agentico custom. ServiceNow con AI for ServiceNow espone i workflow CMDB e ITSM come su- perficie agentica. Anche SAP sta lavorando in questa direzione su S/4HANA.

MCP, A2A e l'interoperabilità che diventa lo standard

Quello che rende possibile l'Headless multi-vendor è una nuova generazione di protocolli di interoperabilità maturata fra il 2024 e il 2026: **Model Context Protocol (MCP)** di Anthropic, per dare a un agente accesso strut- turato a tool e risorse esterne; **Agent-to-Agent (A2A)** di Google, per il coordinamento peer-to-peer fra agenti.

Sono protocolli giovani — MCP è stato proposto a fine 2024, A2A nel 2025 — ma la traiettoria è chiara: nei pros- simi 18-24 mesi diventeranno il sostrato standard dell'in- teroperabilità agentica fra vendor. Headless 360 li adotta esplicitamente: i 60+ MCP tools che Salesforce espone sono il primo passo concreto di una piattaforma enterpri- se che parla il linguaggio standard dei protocolli agentici.

Nel Hype Cycle for Agentic AI 2026, Gartner descrive il 2026 come il breakthrough year per i multi-agent systems e cita MCP come il protocollo che sta definendo gli standard di scambio di contesto fra agenti (Gartner, *Hype Cycle for Agentic AI 2026*).

Il prossimo livello non è una rivoluzione

Headless e i protocolli di interoperabilità non sono una rivoluzione che cambia la direzione complessiva del lavo- ro agentico. Sono uno spostamento del baricentro: dalla piattaforma come SaaS chiuso alla piattaforma come in- frastruttura aperta a componenti esterni.

Significa che la scelta architetturale di oggi va presa con la consapevolezza che, da qui a due anni, i quadranti del capitolo precedente saranno meno rigidi. L'implicazione per chi ha investito in queste piattaforme negli anni è significativa. Il valore accumulato (dati, regole di business, automazioni, integrazioni, processi) non sta nelle schermate, ma nelle logiche e nei dati sottostanti.

Ciò significa che, con il supporto di partner esperti della tecnologia e qualificati, anche i clienti storici Salesforce e altri SaaS potrebbero trasformare il proprio patrimonio applicativo esistente — dati, processi, automazioni, Apex, Flow, integrazioni e logiche di business — in servizi digitali “headless” e agent-ready, utilizzabili da portali, app, canali conversazionali, agenti AI e nuove interfacce leggere, senza dover rifare da zero la piattaforma.

5.1 Cosa serve mettere a terra

Alla luce degli elementi discussi in queste pagine e della nostra esperienza, sia con i casi illustrati precedentemente che con le altre realtà con cui ci interfacciamo, emergono sei elementi non negoziabili per attuare l'Agentic Enterprise.

1. Una scelta architetturale lucida. È la decisione da cui tutto parte. Posizionarsi consapevolmente nella matri- ce del capitolo precedente, scegliere il quadrante (o il mix di quadranti per processo) in funzione dei vincoli normati- vi, del patrimonio informativo esistente, delle competenze interne disponibili, della velocità di go-live attesa. Una scelta da fare guardando al presente, certo, ma soprat- tutto immaginando gli scenari futuri e scegliendo un'archi- tettura che possa evolvere coerentemente.

2. Governance prima della tecnologia. Occorre decide- re chi controlla cosa decide l'agente, dove può agire in autonomia, dove deve passare all'umano, come si traccia ogni decisione. La governance non è solo un documento, è il telaio progettuale su cui il resto si appoggia. Quando la sovranità del dato impone la governance a monte, il vantaggio collaterale è una disciplina che il cloud “default” non costringe a costruire.

3. Knowledge base curata da una persona dedicata. L'investimento principale di un progetto agentico dovrebbe essere la costruzione e manutenzione continua della Knowledge Base su cui questo poggia. Senza qualcuno che la presidi, anche l'agente migliore inciampa sulle stesse risposte. Sia per la PA che per le aziende, una delle lezioni che più spesso vediamo sul campo è che questo aspetto è quello che fa la differenza fra i progetti che funzionano e quelli che non funzionano.

4. Persone interne presidianti. Servono varie figure interne che supportino il progetto e stimolino il cambiamento: uno sponsor di alto livello con potere decisionale, un knowledge manager che abbia responsabilità del patrimonio di informazioni, un project manager con visione operativa fra agente e processi.

5. Un partner che accompagni l'evoluzione. Spesso, però, ciò che fa la differenza è il partner giusto, che affianchi e supporti nella transizione anche nei momenti complessi. Non un vendor che vende un agente in scatola, ma un consulente che sappia indicare la strada in base al livello di maturità della tecnologia e dell'organizzazione, che sappia riposizionarsi quando ci sono difficoltà, che governi la transizione tra le tappe del processo.

6. Visione di lungo termine. Il fine tuning post go-live è parte integrante del progetto, non un'anomalia da risolvere o un errore. Una roadmap a 18-24 mesi è condizione necessaria. Le aziende che pensano al primo go-live come traguardo finale tendono a fermarsi al primo agen- te; quelle che lo trattano come prima tappa di un viaggio organizzativo si dirigono verso l'Agentic Enterprise.

Questi sei elementi sono quelli che abbiamo identificato come risposte alle principali barriere che l'Osservatorio del Politecnico di Milano ha individuato per l'Intelligent Process Automation nelle aziende italiane (competenze, governance, change management, infrastruttura) e sono applicabili a tutte le realtà, pubbliche e private.

Le barriere dell'automazione di processo — intelligente e non

Fonte: Osservatorio Intelligent Business Process Automation, Politecnico di Milano.

Crediti

Il prossimo passo

Vuoi confrontarti sulla tua architettura AI e sulla sua evoluzione in ottica agentica? Contattaci per esplorare le possibilità: **gunpowder.eu/contact/**

Vuoi esplorare Giano o valutare un'implementazione Salesforce-native? Trovi i dettagli su **gunpowder.eu/prodotti/giano** e **gunpowder.eu/storie-di-successo**.

Vuoi restare aggiornato sulle evoluzioni di mercato e sui prossimi White Paper? Seguici su LinkedIn: **linkedin.com/company/gp-gunpowder**

A proposito di Gunpowder

Gunpowder è una tech consultancy italiana e software house specializzata in trasformazione digitale, nata come spin-off dell'Università dell'Aquila. Salesforce Partner Summit dal 2017, Gunpowder è specializzata in CRM, Intelligenza Artificiale, data management e soluzioni cloud. Ha realizzato più di quattrocento progetti in oltre dieci industries — Automotive, Healthcare, Utilities, Financial Services,

Hanno contribuito a questo white paper

- **Ilaria Cazziol** — Content Strategist & Writer
- **Camilla Di Maio** — Marketing & Communication Officer, Gunpowder
- **Davide Iacobelli** — Head of BI & AI Competence Center, Gunpowder
- **Cristina Rimondo** — Sales Manager, Gunpowder
- **Davide Fulcini** — General Market Lines Director, Gunpowder

GUNPOWDER

info@gunpowder.com
www.gunpowder.eu
gunpowder
gunpowder_srl