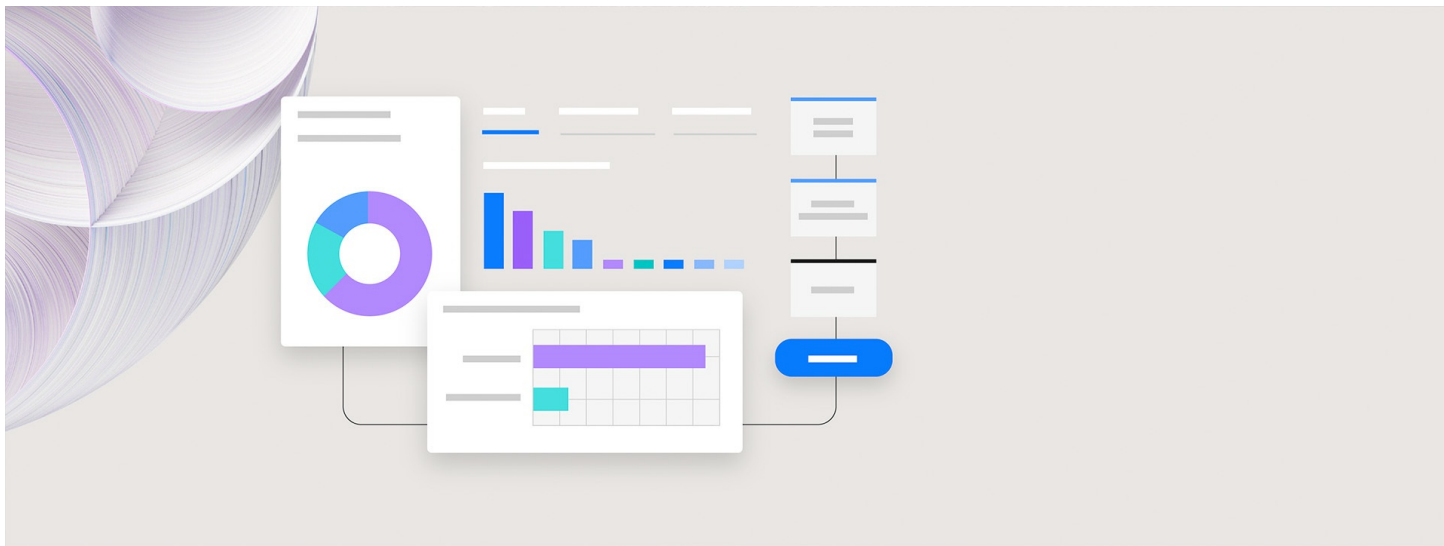


## IBM presenta il primo software del settore per unificare governance degli agenti e sicurezza

- Le nuove integrazioni di IBM aiutano le aziende a mantenere sicuri e responsabili i loro sistemi di AI agentica così come altri sistemi di AI generativa
- Le aziende possono effettuare prove red team degli agenti, audit degli agenti, rilevare agenti “ombra” e molto altro.



ARMONK, N.Y., 18 giugno 2025 /PRNewswire/ -- Oggi, mentre le aziende stanno implementando agenti di intelligenza artificiale in tutte le loro organizzazioni, IBM annuncia il primo software del settore in grado di riunire i team di sicurezza e governance dell'AI e fornire una visione unificata del profilo di rischio delle aziende.

Le nuove capacità arricchiscono e integrano watsonx.governance e Guardium AI Security per aiutare i clienti a mantenere i loro sistemi di intelligenza artificiale, compresi gli agenti, sicuri e responsabili su larga scala. Watsonx.governance è lo strumento IBM di governance end-to-end dell'AI e Guardium AI Security è lo strumento di IBM per proteggere i modelli di intelligenza artificiale, i dati e il loro utilizzo.

*"Gli agenti di intelligenza artificiale sono destinati a rivoluzionare la produttività aziendale, ma i benefici stessi degli agenti di AI possono anche rappresentare una sfida", ha dichiarato Ritika Gunnar, General Manager, Data and AI, IBM "Quando questi sistemi autonomi non sono correttamente gestiti o protetti, possono comportare gravi conseguenze".*

Queste alcune delle novità presentate oggi:

## Unificare e automatizzare la sicurezza dell'AI agentic

IBM migliora l'integrazione tra IBM Guardium AI Security e watsonx.governance, offrendo alle aziende la prima soluzione unificata per gestire i rischi di sicurezza e governance associati ai casi d'uso dell'intelligenza artificiale. L'integrazione supporta i processi degli utenti per validare la conformità verso 12 diversi framework, tra cui l'AI Act UE e l'ISO 42001.

IBM annuncia anche nuove funzionalità per Guardium AI Security attraverso una collaborazione con AllTrue.ai, inclusa la capacità di rilevare nuovi casi d'uso di intelligenza artificiale negli ambienti cloud, repository di codice e sistemi integrati, offrendo ampia visibilità e protezione in un ecosistema di AI sempre più decentralizzato. Una volta identificati, IBM Guardium AI Security può attivare automaticamente da watsonx.governance i workflow di governance appropriati.

I recenti aggiornamenti di IBM Guardium AI Security includono anche il red teaming automatizzato per aiutare le organizzazioni a rilevare e correggere le vulnerabilità e le configurazioni errate in tutti i casi d'uso dell'AI. E per mitigare i rischi come l'iniezione di codice, l'esposizione di dati sensibili e la fuoriuscita di dati, lo strumento consente agli utenti di definire politiche di sicurezza personalizzate che analizzano sia i prompt di input che quelli di output. Queste funzionalità sono già ora disponibili in IBM Guardium AI Security, e la loro integrazione con watsonx.governance verrà rilasciata gradualmente nel corso dell'anno.

*"Il futuro dell'intelligenza artificiale dipende da quanto bene la proteggiamo oggi. Incorporare la sicurezza fin dall'inizio è essenziale per la protezione dei dati, il supporto agli obblighi di conformità e la costruzione di una fiducia duratura",* ha dichiarato **Suja Viswesan, Vice President, Security and Runtime Products, IBM**

*"Uno dei maggiori problemi per i team di sicurezza è tradurre le violazioni di incidenti e conformità in rischi aziendali quantificabili. L'adozione rapida dell'intelligenza artificiale e dell'AI agentic amplifica questo problema",* ha dichiarato **Jennifer Glenn, Research Director for the IDC Security and Trust Group**. *"Unificare la governance e la sicurezza dell'intelligenza artificiale dà alle organizzazioni il contesto necessario per identificare e dare priorità ai rischi, oltre ad avere le informazioni per comunicare chiaramente le conseguenze del non affrontarli".*

## Valutazione dell'AI e governance del ciclo di vita

IBM watsonx.governance può ora monitorare e gestire gli agenti di AI durante tutto il loro ciclo di vita, dalla fase di sviluppo alla

fase di rilascio. I nodi di valutazione possono essere costruiti direttamente negli agenti, consentendo agli utenti di monitorare con cura metriche come la rilevanza delle risposte, la rilevanza del contesto e la fedeltà – e aiutarli a identificare la causa primaria delle basse performance. Le funzionalità a piano per il futuro includono la valutazione dei rischi legati dell'inserimento degli agenti, i percorsi di audit degli agenti e un catalogo di strumenti agentici, che dovrebbero essere disponibili dal 27 giugno.

## **Funzionalità di conformità pronte all'uso**

IBM watsonx.governance Compliance Accelerators fornisce regolamenti, standard e framework da tutto il mondo, selezionati e pre-caricati, consentendo agli utenti di identificare quali siano gli obblighi pertinenti e di mapparli sui propri casi d'uso di AI. Il contenuto tratta le normative principali come l'AI Act UE, la SR 11-7 della U.S. Federal Reserve e la Local Law 144 di New York City, oltre a standard globali come l'ISO/IEC 42001 e framework come il NIST AI RMF. Watsonx.governance Compliance Accelerators è ora disponibile come opzione aggiuntiva.

Per fornire maggiore valore ai clienti AWS, watsonx.governance è ora disponibile anche nel datacenter di AWS in India con funzionalità avanzate di monitoraggio dei modelli.

Le odierne nuove capacità e integrazioni forniscono alle aziende la governance e la sicurezza complete di cui hanno bisogno per avere successo nell'era dell'intelligenza artificiale agentica. Le innovazioni sono in linea con il più ampio portfolio di soluzioni AI IBM watsonx, progettate per aiutare le aziende ad accelerare l'impatto dell'intelligenza artificiale generativa in modo responsabile e sicuro.

## **IBM**

IBM è un'azienda leader a livello mondiale di cloud ibrido, intelligenza artificiale e competenze di consulenza e opera con le imprese di oltre 175 Paesi aiutandole a capitalizzare sugli insight dei loro dati, a semplificare i processi aziendali, a ridurre i costi e a ottenere un vantaggio competitivo nei loro settori d'industria. Quasi 4.000 enti governativi e aziende in aree infrastrutturali critiche come quelle dei servizi finanziari, delle telecomunicazioni e sanità si affidano alla piattaforma cloud ibrida di IBM e a Red Hat OpenShift per realizzare la loro trasformazione digitale in modo rapido, efficiente e sicuro. Le innovazioni di IBM nell'ambito dell'AI, del quantum computing, delle soluzioni cloud specifiche per settore d'industria e nella consulenza sono offerte con opzioni open e flessibili. Tutto questo è supportato dal ben noto impegno di IBM per la trasparenza, la responsabilità, l'inclusività e il servizio. Per maggiori informazioni, visitate il sito [ibm.com/it-it](https://ibm.com/it-it)

LinkedIn: [IBM](#)

Contatti:

**Titti Garau** - *External Relations, IBM Italy*

email: [titti\\_garau@it.ibm.com](mailto:titti_garau@it.ibm.com)

mobile: 335 7248411

---