CYBER & SECURITY SOLUTIONS

FORGE2KNOW
AI ENGINE

MODELLI AI AFFIDABILI
RESPONSABILI E CONFORMI

LEONARDO

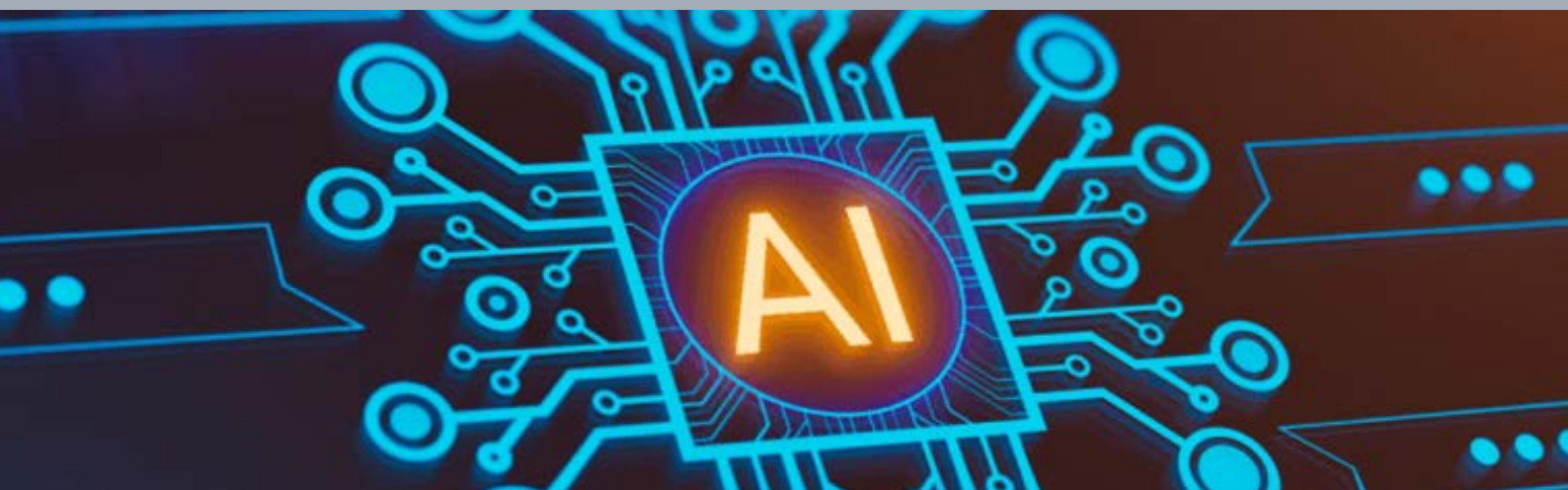
Governi, aziende e organizzazioni riconoscono i dati come una risorsa preziosa in grado di offrire conoscenza, guidare il processo decisionale e migliorare le prestazioni complessive dei processi aziendali.
Leonardo ha progettato la suite Forge2Know per affrontare le sfide dell'analisi integrata dei Big Data e della governance dell'Intelligenza Artificiale.
Strutturata con 2 prodotti interoperabili ma indipendenti, Forge2Know integra moderne tecnologie open source e moduli proprietari, progettati per garantire sicurezza, scalabilità e interoperabilità in ambienti diversi.

Forge2Know.DataPlatform
Una piattaforma costituita da strumenti per velocizzare e semplificare la governance dei dati, acquisizione, elaborazione e presentazione di Big Data.

Forge2Know.AIEngine
Una piattaforma per la governance dei modelli di AI in termini di: Responsible AI, Repository (Model/Dataset), Distribuzione, Monitoraggio Attivo, Raccolta delle esperienze e Valutazione dei Benchmark.

I due prodotti Forge2Know possono essere utilizzati come soluzioni stand-alone, ciascuna pienamente operativa e allo stesso tempo sono complementari per ottenere una piattaforma completa e scalabile che consente di trasformare i dati in valore strategico, ottimizzando la governance, l'elaborazione e l'adozione dell'Intelligenza Artificiale con elevati standard di sicurezza e interoperabilità.

Entrambi i prodotti rappresentano la piattaforma abilitante per **Forge2Know.DataIntelligence**, una soluzione avanzata che integra strumenti di crawling e l'uso evoluto dell'Intelligenza Artificiale per l'analisi OSINT e CLOSINT, consentendo la raccolta, l'elaborazione e l'analisi di grandi quantità di dati provenienti da fonti aperte e chiuse, a supporto dei processi decisionali.



Negli attuali scenari applicativi Big Data e Intelligenza Artificiale sono spesso usati congiuntamente per poter gestire l'enorme quantità di dati da trattare, velocizzarne l'elaborazione e assicurare la completezza dell'analisi. Questo sta determinando una crescente domanda di soluzioni dove i diversi modelli devono essere fruiti in modo cooperativo e sicuro all'interno di piattaforme di erogazione in grado di assicurare i requisiti prestazionali. È universalmente accettato che accanto agli indubbi benefici, l'utilizzo della AI aumenta il rischio di sicurezza e determina la necessità di ambienti in grado di garantire la governance, l'affidabilità, la correttezza, la sicurezza, la privacy e la protezione dei dati e dei modelli AI.

Leonardo nell'ambito della suite Forge2Know (F2K) per la valorizzazione dei dati, ha progettato e realizzato la piattaforma Forge2Know.AIEngine che offre i servizi per la governance, la protezione e la sicurezza dei modelli di AI, composta da un repository centralizzato e da servizi di erogazione, monitoraggio e raccolta dell'esperienza, con un forte focus sulla conformità normativa (es. Responsible AI, AI Act) e sulla sicurezza tecnica (es. Secure AI, AI Safety).

La piattaforma può essere utilizzata in modalità stand-alone ed essere complementare a Forge2Know. DataPlatform che fornisce strumenti per la governance, l'ingestion, il processing dei Big Data e la loro presentazione costituendo un ecosistema all'avanguardia per la valorizzazione dei dati usufruibile in modalità on premise o PaaS/SaaS (Platform as a Service/Software as a Service).

CARATTERISTICHE PRINCIPALI

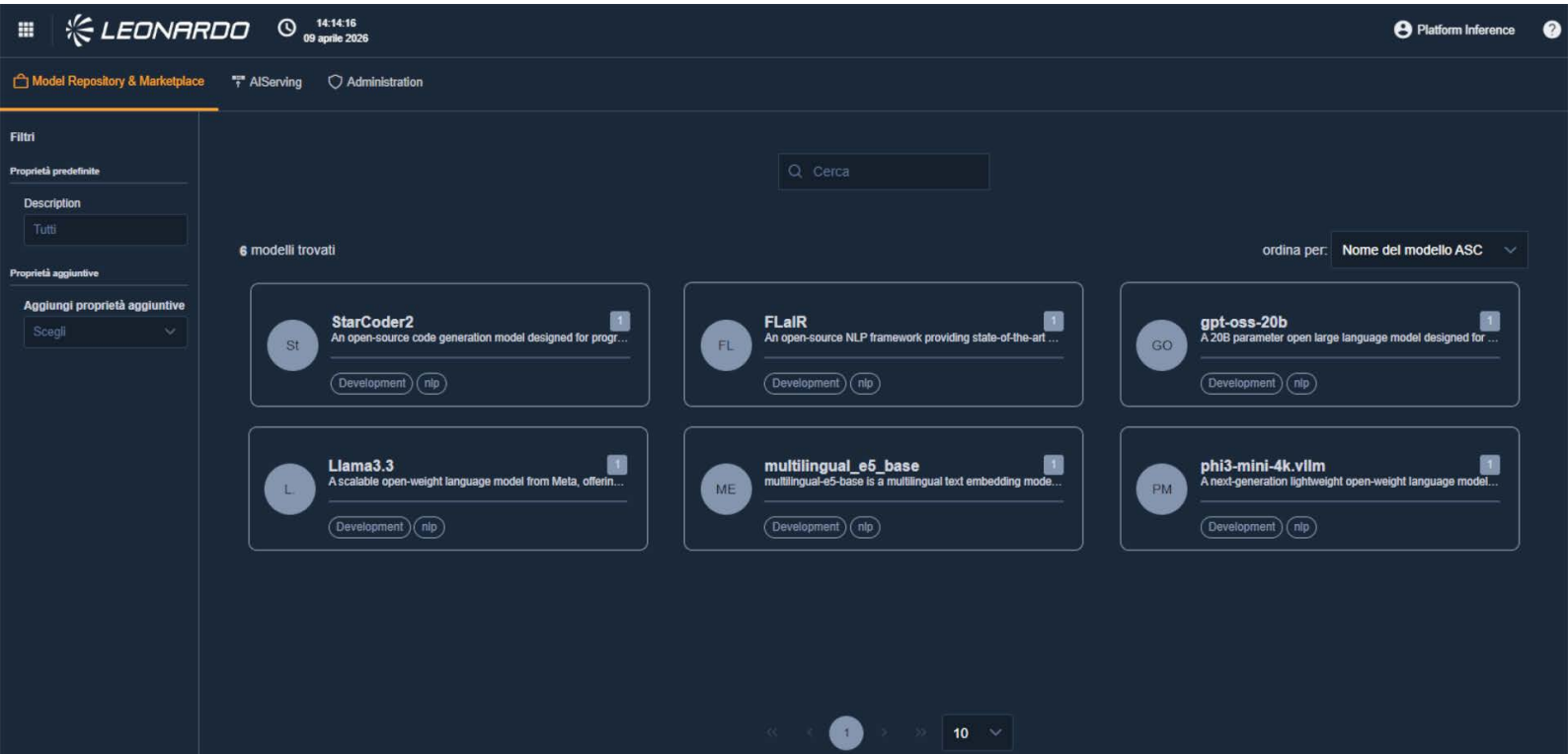
Forge2Know.AIEngine gestisce i modelli di AI in termini di repository, erogazione, monitoraggio attivo e benchmarking attraverso una serie di moduli cooperanti che realizzano le seguenti funzionalità:

- → Repository (Model/Dataset): Archiviazione, Versioning, Model Card, Tracking.
- → Serving di inferenze e pipeline di inferenze nella forma centralizzata, decentralizzata online e decentralizzata offline.
- → Active Monitoring: capacità di monitorare e controllare lo stato di operatività dei modelli e dei nodi/host.
- → Benchmark Evaluation: strumenti per la valutazione delle performance dei modelli in inferenza.
- → Experience Collector: strumenti per la raccolta della experience durante il serving dei modelli.

Forge2Know.AIEngine è progettata per garantire la protezione del dato e la sicurezza dei modelli.

La piattaforma è dotata di strumenti per:

- → Per garantirne l'identità e l'integrità dei modelli AI.
- → Validazione del modello con livello di rating sulla vulnerabilità (AI Security).
- → Supporto alla verifica della conformità alla normativa europea sull'Intelligenza Artificiale (AI Act).
- → Supporto alla Responsible AI, per garantire un utilizzo etico, trasparente e controllato dei modelli di Intelligenza Artificiale.



FUNZIONALITÀ E SERVIZI

Forge2Know.AIEngine è progettato e realizzato per offrire un'ampia gamma di funzionalità avanzate e intelligenti per la gestione dei modelli AI.

REPOSITORY

È il fondamento della governance dei modelli e si occupa principalmente di gestire:

- → ARCHIVIAZIONE DEI MODELLI AI sviluppati da Leonardo e/o da terze parti.
- → ARCHIVIAZIONE DEI DATASET utilizzati per l'addestramento e benchmark dei modelli.
- → CERTIFICAZIONE DELLE PIPELINE da associare ai modelli.
- → VERSIONING AVANZATO di modelli e Dataset.
- → MODEL CARD, contenente:
  - → Autore, data e origine del modello
  - → Descrizione e origine del Dataset utilizzato per l'addestramento
  - → Manifesto di Cyber Resilience che racchiude, raccoglie e rileva metriche a supporto delle verifiche di compliance normative, tecniche ed etiche (AI Act, AI Security, Responsible AI) per ogni singola versione.
- → DATASET CARD, contenente:
  - → Autore, data e origine del Dataset
  - → Descrizione e schema delle caratteristiche
  - → Modelli associati al Dataset
  - → Report di qualità dei dati
- → TRACKING dei download e dei deployment.

SERVING

Trasforma il modello AI da asset "statico" a servizio operativo di business, abilitando l'inferenza e pipeline di inferenza con possibilità flessibile di erogazione in diverse modalità (centralizzata, decentralizzata online e edge/ offline):

CENTRALIZZATA

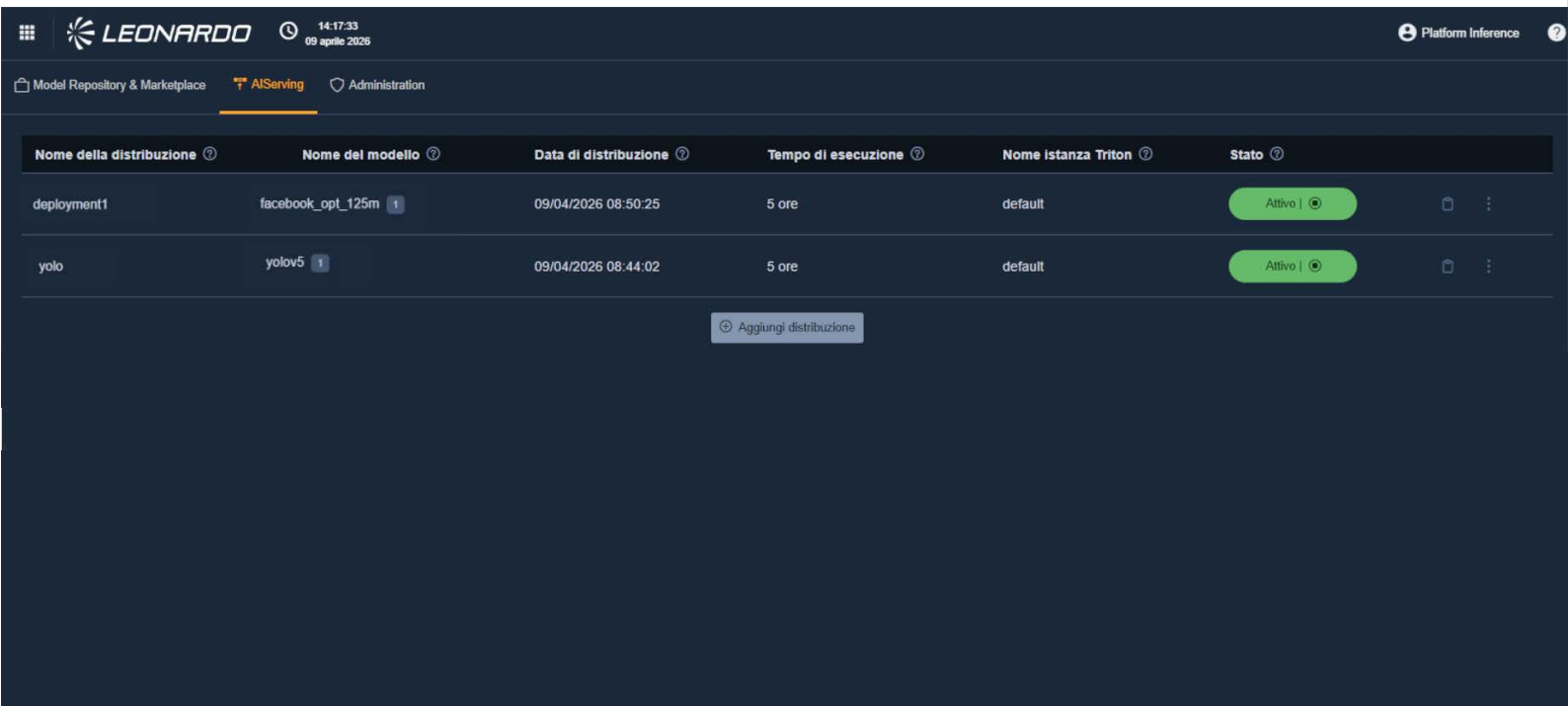
Nella modalità centralizzata le richieste di inferenza sono elaborate dal server centrale, sfruttando la gestione centralizzata delle risorse e la scalabilità della piattaforma. È possibile distribuire i carichi di lavoro su più nodi, scegliendo il dimensionamento ottimale per garantire efficienza e performance elevate nella gestione delle inferenze.

DECENTRALIZZATA (ON EDGE) CONNESSA

Nella modalità decentralizzata, la piattaforma consente alle istanze locali di eseguire l'inferenza dei modelli direttamente su macchine e dispositivi distribuiti, estendendo così una componente minima di serving anche sui nodi edge. La piattaforma centrale continua a gestire metadati, metriche e configurazioni, garantendo coordinamento e monitoraggio centralizzato. Le istanze locali si sincronizzano regolarmente con il server centrale per assicurare l'aggiornamento di modelli e configurazioni e per recuperare i dati necessari al corretto funzionamento della piattaforma.

DECENTRALIZZATA (ON EDGE) NON CONNESSA

Nella modalità decentralizzata disconnessa, la piattaforma consente comunque alle istanze locali di eseguire l'inferenza dei modelli direttamente su macchine e dispositivi, ma in modalità non automatica, mediante il deploy manuale di una componente minima di serving. La piattaforma centrale continua a gestire metadati, metriche e configurazioni, garantendo coordinamento e monitoraggio centralizzato. Le istanze locali non dispongono di meccanismi di sincronizzazione automatica, ma prevedono comunque strumenti per la raccolta di dati e metriche in modalità offline.



MONITORING, BENCHMARK EVALUATION & EXPERIENCE COLLECTOR

Modulo funzionale che fornisce la capacità di monitorare e controllare lo stato di operatività dei modelli e dei nodi/host e offre gli strumenti per raccogliere i dati (experience) sia per misurare le performance che per futuri addestramenti.

Per ogni inferenza eseguita ed identificata, è possibile raccogliere i valori di input, output e rilevato attraverso due modalità:

- API: il valore rilevato sarà iniettato via API (da sistemi terzi).
- HMI: Il valore rilevato sarà iniettato via HMI (con strumenti di import automatici).

È un elemento fondamentale della governance per avere sotto controllo data drift e concept drift, performance reali vs attese, bias e fairness nel tempo, anomalie operative (latenza, errori, outlier).

La piattaforma offre un'interfaccia web innovativa e user-friendly, pensata per tutti gli utenti coinvolti nella gestione dei modelli AI, dai tecnici ai decisori non tecnici. Progettata per semplificare la compliance normativa sull'AI, ridurre i rischi di sicurezza, accelerare il deploy e ottimizzare le risorse, permette di trasformare i modelli AI in servizi operativi in modo semplice ed efficace.

L'INTEGRAZIONE CON LA PIATTAFORMA BIG DATA

Trasforma il modello AI da asset "statico" a servizio operativo di business, abilitando l'inferenza e pipeline di inferenza con possibilità flessibile di erogazione in diverse modalità (centralizzata, decentralizzata online e edge/offline):

L'uso combinato della Data Platform e dell'AI Engine nella suite Forge2Know moltiplica le capacità del singolo prodotto e consente di creare un ambiente flessibile, sicuro ed efficiente per estrarre valore dai dati.
La DataPlatform dispone di tutti gli strumenti per creare un modello AI e di eseguirne il training.

Il modello creato viene archiviato nel repository dell' AI Engine insieme con i dati di training e tutte le informazioni accessorie per valutarne la sicurezza e l'aderenza alle politiche richieste.

Il modello così inserito è a disposizione, unitamente ad altri modelli, anche di terze parti, presenti nel repository per essere utilizzato dalle varie figure professionali che necessitano di supporti AI per la loro attività.

Se e quando tali attività necessitino di inferenze il ricorso al modulo di Serving permette, nelle diverse modalità previste dalla piattaforma, l'esecuzione dei modelli e la raccolta dei risultati che possono essere utilizzati dagli opportuni strumenti di visualizzazione o trasferiti in altre piattaforme di livello superiore per eventuali ulteriori elaborazioni.

CASI D'USO

La piattaforma consente di utilizzare tecniche di AI in diversi settori applicativi mediante la gestione e l'erogazione di:

- modelli SLM/LLM foundational
- modelli di analisi audio/video
- modelli per analisi satellitare nello spettro visibile e iperspettrale
- modelli di forecasting
- modelli per il monitoraggio globale (gestione rischi naturali ed ambientali)

FOCUS SULLA SICUREZZA

La sicurezza dei modelli è fondamentale per sfruttare pienamente la potenzialità dell'Intelligenza Artificiale. La piattaforma mette a disposizione all'interno dei moduli componenti, tutti gli strumenti per poter verificare e controllare un modello: dalle informazioni dettagliate sull'anagrafica, al tracciamento delle varie versioni e dei relativi utilizzi.

È inoltre possibile controllare la rispondenza del modello ai requisiti di sicurezza previsti dalle normative vigenti (AI Act, AI security rating)

Forge2Know.AIEngine consente inoltre di valutare i modelli nel contesto dell'utilizzo etico, consapevole e sostenibile della Intelligenza Artificiale verificando ad esempio la presenza di polarizzazioni (bias) o la trasparenza e la comprensibilità all'utenza.

L'ambiente di sviluppo dei modelli AI (contenuto nella Data Platform):

- → permette la protezione dei dati sensibili e i flussi di lavoro dell'IA secondo elevati standard di sicurezza e riservatezza;
- → impedisce l'esposizione di dati sensibili;
- → garantisce la riservatezza dei dati anche durante l'uso;
- → crea un ambiente di valutazione dell'IA basato sul modello "zero-trust".

VANTAGGI

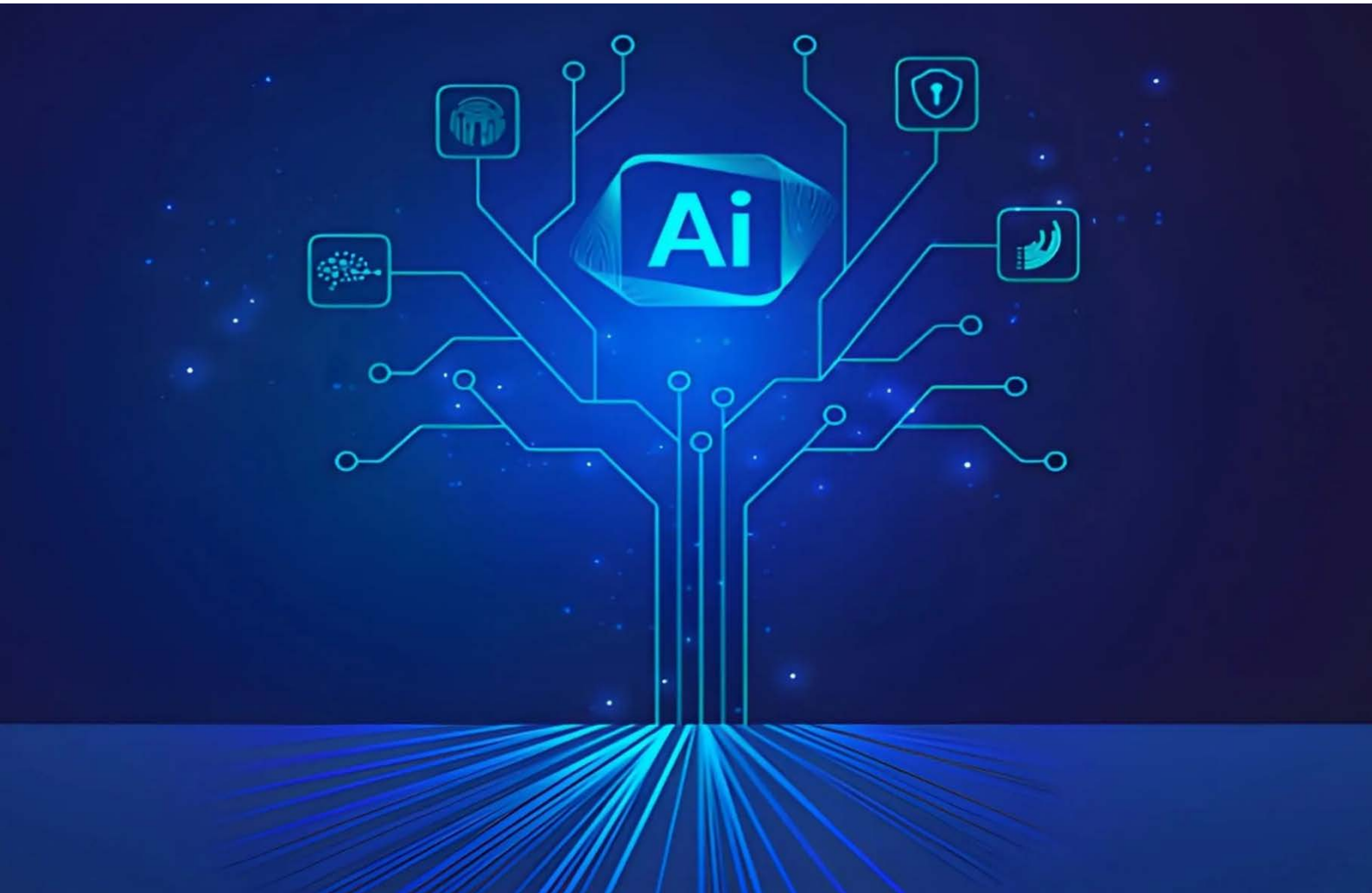
CONTROLLO DEL RISCHIO END-TO-END
La piattaforma garantisce piena tracciabilità e monitoraggio continuo dei modelli in produzione, riducendo rischi operativi, normativi e reputazionali. Il rischio AI passa da evento imprevedibile a elemento governabile e misurabile.

AI SCALABILE E INDUSTRIALIZZATA
Standardizzando repository, serving e valutazione, i modelli diventano asset riusabili e governati, non più soluzioni isolate. Questo consente di scalare l'AI in modo sostenibile, mantenendo velocità di delivery e controllo dei costi.

PERFORMANCE AFFIDABILI NEL TEMPO
Il monitoraggio attivo e il feedback degli utenti permettono di intercettare drift, degrado e bias in tempo reale. I modelli migliorano continuamente, garantendo prestazioni stabili e allineate agli obiettivi di business.

ALLINEAMENTO TRA BUSINESS E COMPLIANCE
Un'unica piattaforma rende trasparenti decisioni, metriche e responsabilità lungo tutto il ciclo di vita del modello. Il risultato è una collaborazione più fluida tra funzioni e processi decisionali più rapidi e informati.

INNOVAZIONE RESPONSABILE E AFFIDABILITÀ NELL'AI
La governance integrata abilita sperimentazione e adozione di modelli avanzati (anche generativi) in totale sicurezza. Più controllo significa più fiducia, e più fiducia accelera l'innovazione.



VALORI CHIAVE

TRASPARENZA	Ogni modello, dato e decisione è tracciabile lungo tutto il ciclo di vita, dal training alla produzione. Questo rende l'AI comprensibile, auditabile e governabile anche in contesti complessi.
CONTROLLO	Policy di deploy, monitoraggio continuo e meccanismi di rollback garantiscono che i modelli operino sempre entro limiti definiti. Il comportamento dell'AI rimane sotto controllo anche in presenza di cambiamenti nei dati o nel contesto.
AFFIDABILITÀ	Il monitoraggio delle performance reali e dei fenomeni di drift assicura risultati stabili nel tempo. I modelli mantengono coerenza con gli obiettivi di business anche in scenari dinamici.
RESPONSABILITÀ	Ruoli, ownership e processi decisionali sono chiaramente definiti e documentati. Ogni scelta è attribuibile, verificabile e allineata alle policy aziendali e regolatorie.
SOSTENIBILITÀ	La piattaforma abilita un'evoluzione continua, sicura e duratura delle soluzioni AI.
FLESSIBILITÀ	Possibilità di operare on-premise, in cloud o in infrastrutture ibride.

For more information:
cyberandsecurity@leonardo.com

Leonardo Cyber & Security Solutions Division
Via R. Pieragostini, 80 - Genova 16151 - Italy

LDO_IT01877 04-26

leonardo.com