CYBER & SECURITY SOLUTIONS

# FORGE2KNOW
## AI ENGINE

RELIABLE RESPONSIBLE AND COMPLIANT AI MODELS

LEONARDO

Governments, businesses, and organizations recognize data as a precious resource capable of offering insights, guiding decision-making, and enhancing the overall performance of business processes.

Leonardo designed the Forge2Know suite to address the challenges of integrated Big Data analytics and Artificial Intelligence governance.

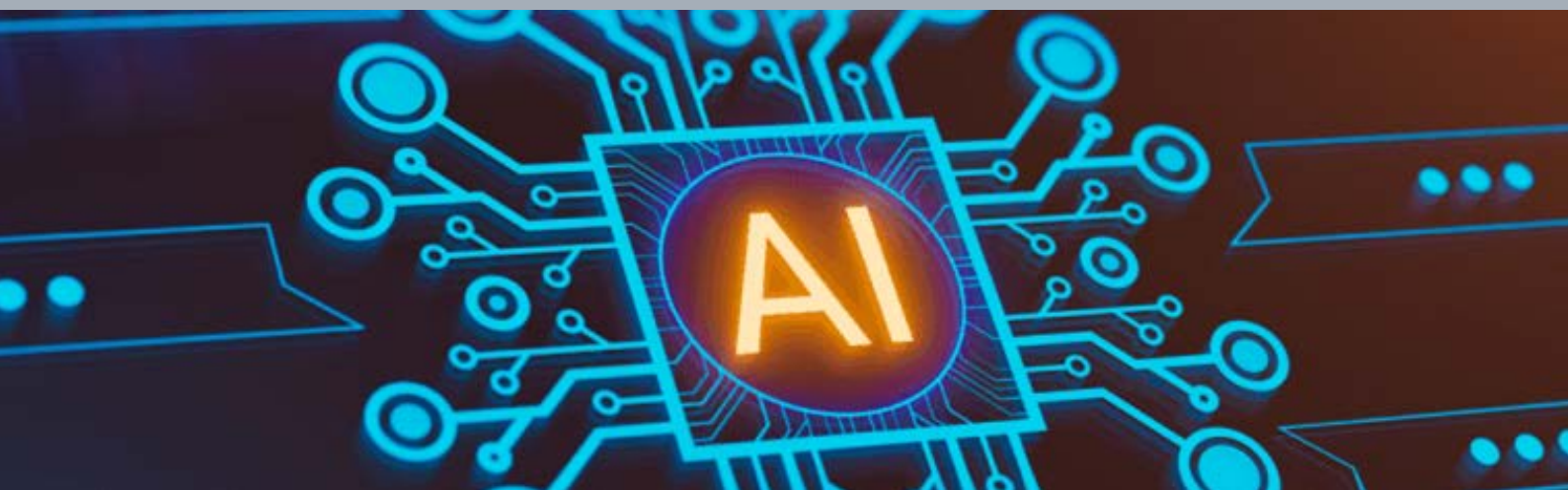
Structured with 2 inter-operating but independent products, Forge2Know integrates modern open-source technologies and proprietary modules, designed to ensure security, scalability and interoperability across environments.

**Forge2Know.DataPlatform**
A platform containing tools to speed up and simplify Big Data governance, acquisition, processing and presentation.

**Forge2Know.AIEngine**
A platform for the governance of AI models in terms of: Responsible AI, Repository (Model/Dataset), Distribution, Active Monitoring, Experience Collection, Benchmark Evaluation.

The two Forge2Know products can be used as fully operational standalone solutions, yet they complement each other to create a comprehensive and scalable platform that enables data transformation into strategic value, optimizing governance, processing and AI adoption with high standards of security and interoperability.

Both products constitute the enabling platform for **Forge2Know.DataIntelligence**, a cutting-edge solution that integrates crawling tools and advanced use of AI for OSINT and CLOSINT analysis enabling the collection, processing and analysis of large amounts of data from open or closed sources to support decisional processes.



In current application scenarios, Big Data and artificial intelligence are often used together to manage the enormous amount of data to be processed, speed up its processing, and ensure the completeness of the analysis. This is driving a growing demand for solutions where different models must be used cooperatively and securely within delivery platforms capable of ensuring performance requirements.

It is universally accepted that, alongside its undoubted benefits, the use of AI increases security risks and creates the need for environments capable of guaranteeing governance, reliability, correctness, security, trustworthiness, privacy, and protection of data and AI models.

As part of its Forge2Know (F2K) suite for data valorization, Leonardo designed and implemented the Forge2Know.AIEngine platform, which offers services for the governance, protection, and security of AI models. The platform consists of a centralized repository and services for delivery, monitoring, and experience collection, with a strong focus on regulatory compliance (e.g., Responsible AI, AI Act) and technical security (e.g., Secure AI, AI Safety).

The platform can be used in stand-alone mode and complement Forge2Know.Data Platform that provides tools for the governance, ingestion, processing and presentation of Big Data, constituting a cutting-edge ecosystem for data valorization that can be used in on-premise or PaaS/SaaS (Platform as a Service/Software as a Service) mode.

## MAIN FEATURES

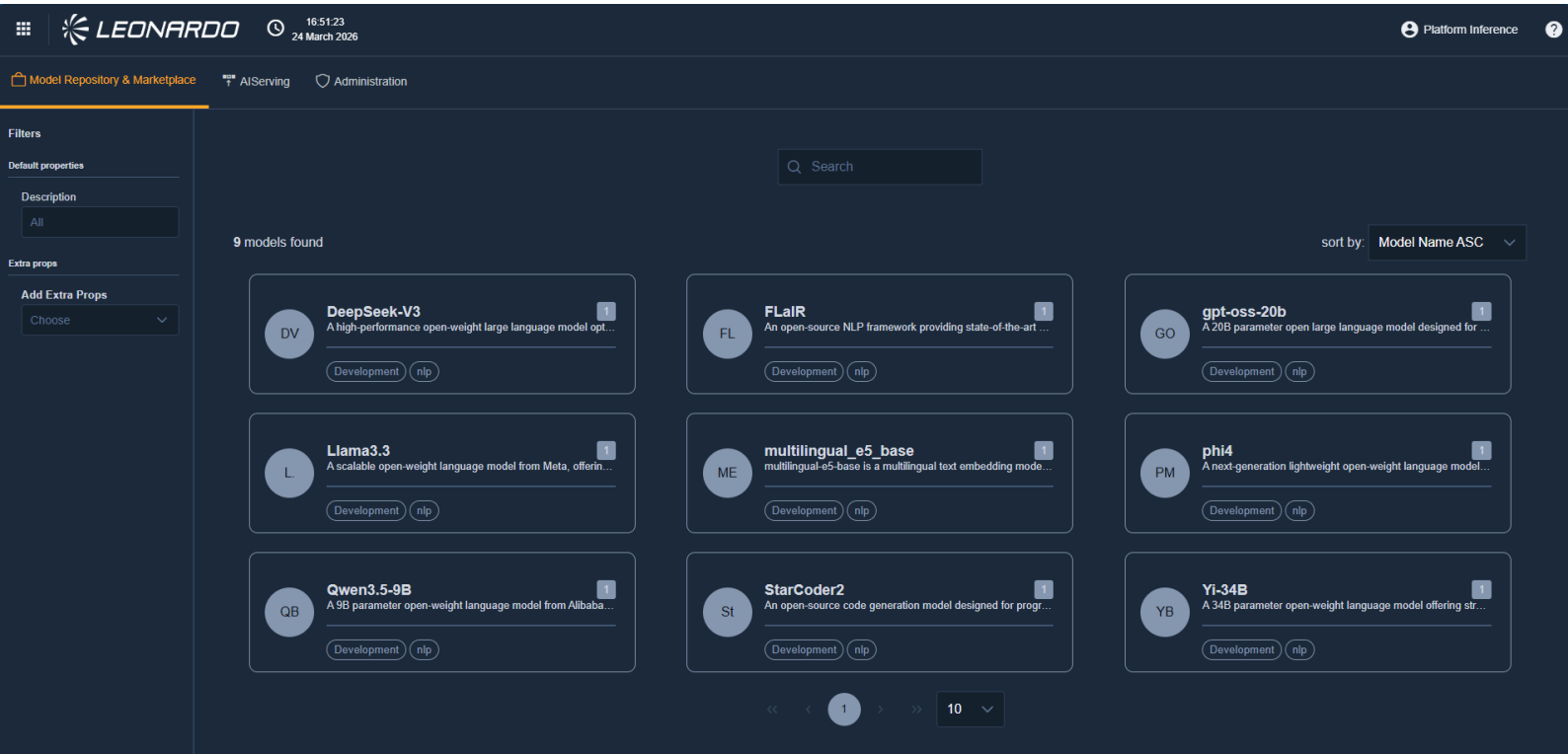
Forge2Know.AIEngine manages AI models in terms of repository, delivery, active monitoring and benchmarking through a series of cooperating modules that achieve the following functionalities:

- → Repository (Model/Dataset): Archival, Versioning, Model Card, Tracking,
- → Inference Serving and Inference Pipelines in centralized, decentralized online and decentralized offline mode.
- → Active Monitoring: ability to monitor and check the operational status of models and nodes/hosts.
- → Benchmark Evaluation: tools for evaluating the performance of inference models.
- → Experience Collector: tools for collecting experience during model serving.

Forge2Know.AIEngine is designed to ensure data protection and model security.

The platform is equipped with tools for:

- → Ensuring the identity and integrity of AI models.
- → Model validation with rating level on vulnerability (AI Security).
- → Support for verifying compliance with the European legislation on artificial intelligence (AI Act).
- → Support for Responsible AI to ensure an ethical, transparent and controlled use of artificial intelligence models.



# SERVICES AND FUNCTIONALITIES

Forge2Know.AIEngine is designed and built to deliver a wide range of advanced and intelligent capabilities for managing AI models.

## REPOSITORY

It is the foundation of model governance and is primarily concerned with managing:

- AI MODELS ARCHIVAL for both Leonardo and/or third parties developed models.
- DATASET ARCHIVAL related to datasets used for models training and benchmarking.
- PIPELINE CERTIFICATION to be associated with the models.
- ADVANCED VERSIONING of models and Datasets.
- MODEL CARD, containing:
  - Author, date and origin of the model
  - Description and origin of the dataset used for the training
  - Cyber Resilience Manifesto which includes, collects and tracks metrics to support regulatory, technical, and ethical compliance checks (AI Act, AI Security, Responsible AI) for each individual version.
- DATASET CARD, containing:
  - Author, date and origin of the model
  - Description and characteristics diagram
  - Models associated with the dataset
  - Data Quality Report
- TRACKING of downloads and deployments.

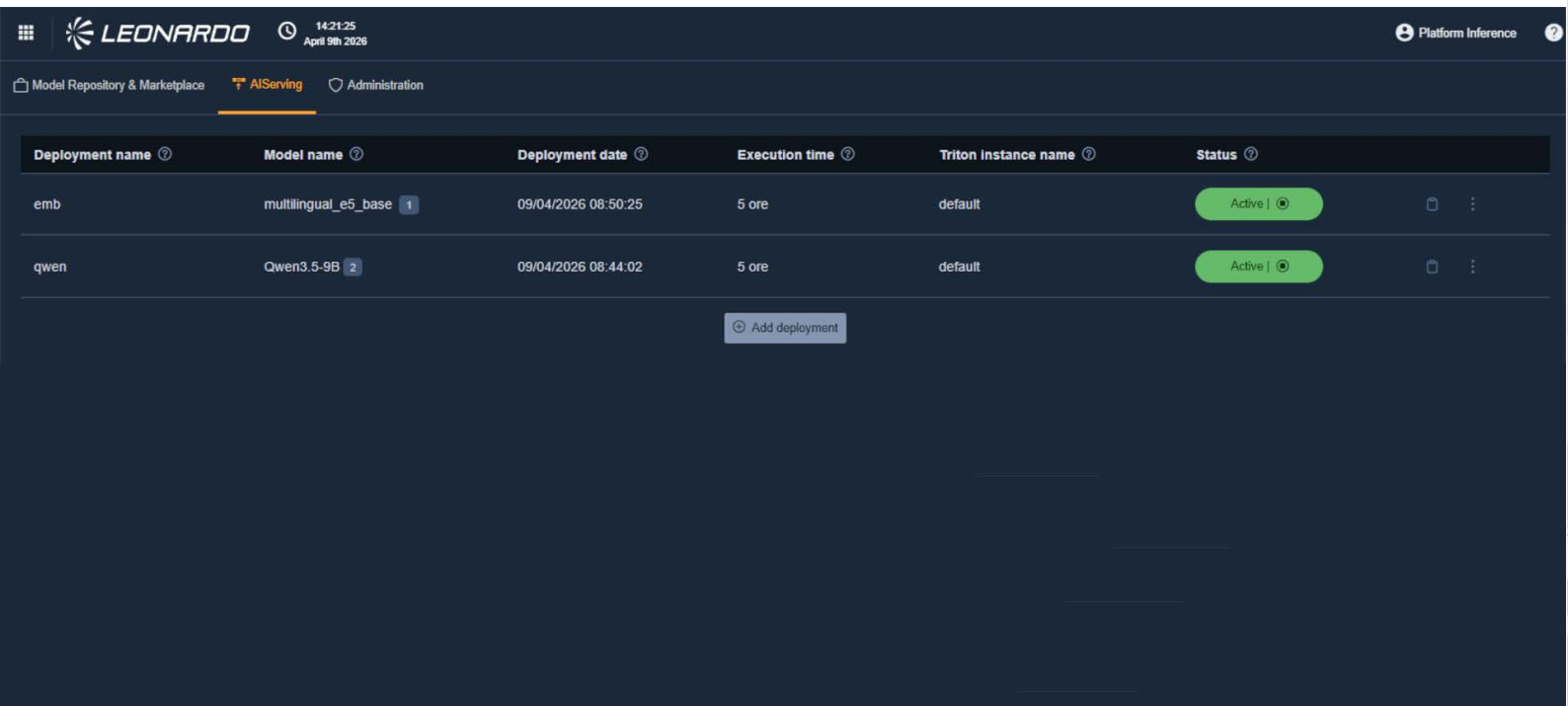
## SERVING

Transforms the AI model from a "static" asset to an operational business service, enabling inference and inference pipelines with flexible delivery options in different modes (centralized, decentralized online and edge/offline):

**CENTRALIZED**
In centralized mode, inference requests are processed by the central server, leveraging centralized resource management and platform's scalability. Workloads can be distributed across multiple nodes, choosing the optimal size to ensure efficiency and high performance in inference management.

**DECENTRALIZED (ON EDGE) CONNECTED**
In decentralized mode, the platform allows local instances to run model inference directly on distributed machines and devices, thus extending a minimal serving component to edge nodes.
The central platform continues to manage metadata, metrics, and configurations, ensuring centralized coordination and monitoring.
Local instances regularly synchronize with the central server to ensure model and configuration updates and to retrieve the data necessary for the platform's proper functioning.

**DECENTRALIZED (ON EDGE) NOT CONNECTED**
In disconnected decentralized mode, the platform still allows local instances to run model inference directly on machines and devices, but in a non-automated manner, through the manual deployment of a minimal serving component.
The central platform continues to manage metadata, metrics, and configurations, ensuring centralized coordination and monitoring.
Local instances lack automatic synchronization mechanisms, but they still provide tools for offline data and metrics collection.



## MONITORING, BENCHMARK EVALUATION & EXPERIENCE COLLECTOR

Functional module that provides the ability to monitor and control the operational status of models and nodes/host and offers the tools to collect data (experience) both to measure performance and for future training.

For each performed and identified inference, it is possible to collect the input, output and detected values in two ways:

- API: the detected value will be injected via API (by third party systems)
- HMI: the detected value will be injected via HMI (with automatic import tools)

It is a fundamental element of governance to keep data drift and concept drift under control, actual vs. expected performance, bias and fairness over time, and operational anomalies (latency, errors, outliers).

The platform offers an innovative and user-friendly web interface, designed for everyone involved in managing AI Models, from technicians to non-technical decision makers.
Designed to simplify AI regulatory compliance, reduce security risks, accelerate deployment, and optimize resources, it allows AI models to be transformed into operational services in a simple and effective way.

## BIG DATA PLATFORM INTEGRATION

Transforms the AI model from a "static" asset to an operational business service, enabling inference and inference pipelines with flexible delivery options in different modes (centralized, decentralized online and edge/offline):

The combined use of the Data Platform and the AI Engine in the Forge2Know suite multiplies the capabilities of the single product and allows you to create a flexible, secure and efficient environment for extracting value from data. The DataPlatform has all the tools to create and train an AI model.

The created model is stored in the AI Engine repository along with the training data and all the ancillary information to evaluate its security and compliance with the required policies.

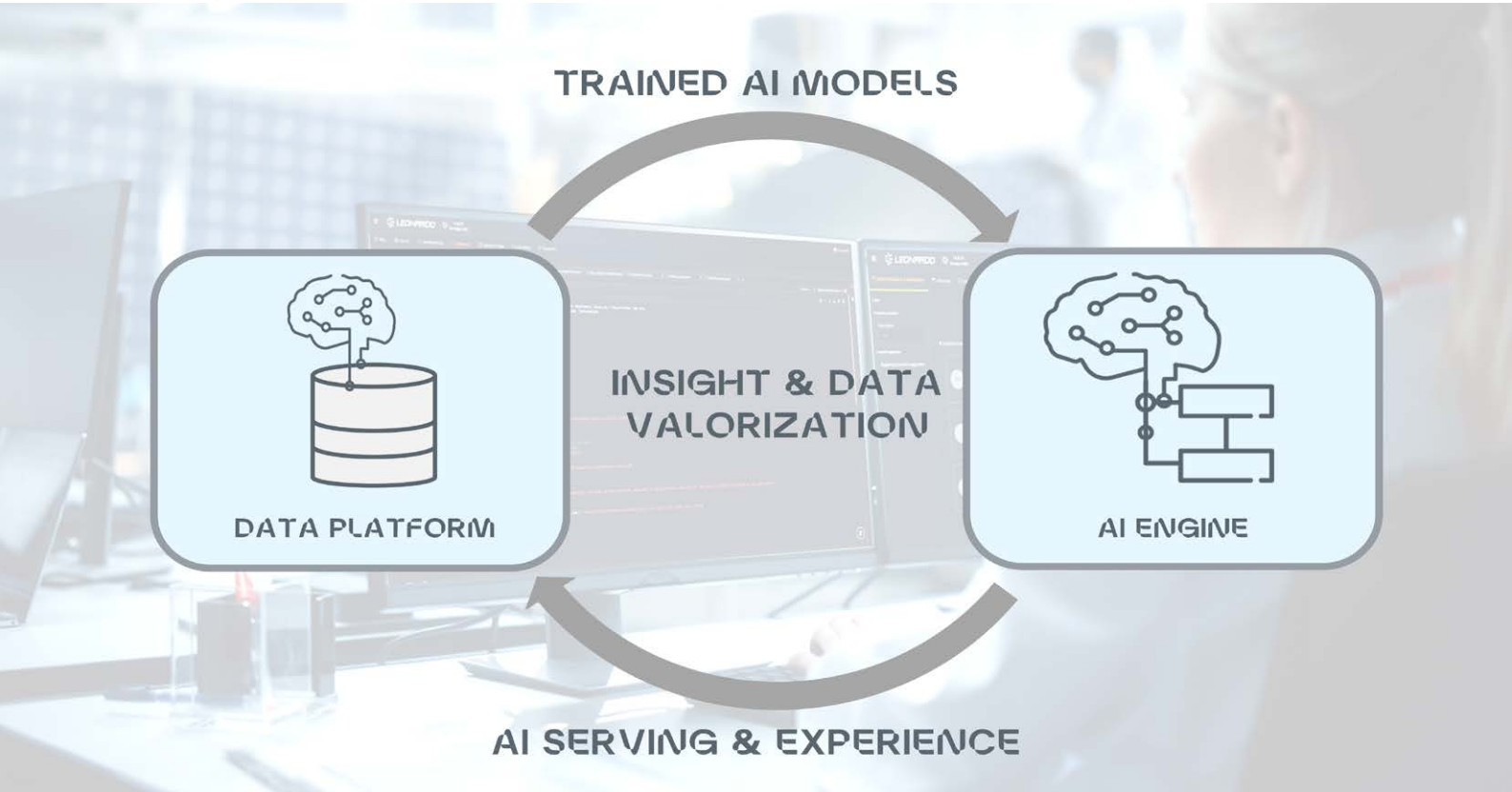
The model thus inserted is made available, together with other models including third-party ones, within the repository, to be utilized by various professionals who require AI support for their activities.

If and when these activities require inferences, resorting to the Serving module allows, through the various mechanisms provided by the platform, the execution of the models and the collection of results that can be used by the appropriate visualization tools or transferred to other higher-level platforms for any further processing.

## USE CASES

The platform allows the use of AI techniques in various application sectors through the management and delivery of:

- SLM/LLM foundational models
- audio/video analysis models
- models for satellite analysis in the visible and hyper-spectral spectrum
- forecasting models
- models for global monitoring (management of natural and environmental risks)



## FOCUS ON SECURITY

Model security is essential to fully exploit the potential of Artificial Intelligence.
The platform provides all the tools needed to verify and control a model within its component modules: from detailed information on the master data to tracking the various versions and their relative uses.

It is also possible to check the model's compliance with the security requirements set by current regulations (AI act, AI security rating).

Forge2Know.AIEngine also allows you to evaluate models in the context of the ethical, conscious and sustainable use of Artificial Intelligence by verifying, for example, the presence of biases or transparency and comprehensibility to users.

The AI model development environment (contained in the Data Platform):

- → enables the protection of sensitive data and AI workflows in accordance with high standards of security and confidentiality;
- → prevents the exposure of sensitive data;
- → guarantees data confidentiality even during use;
- → creates an AI evaluation environment based on the zero-trust model.

## ADVANTAGES

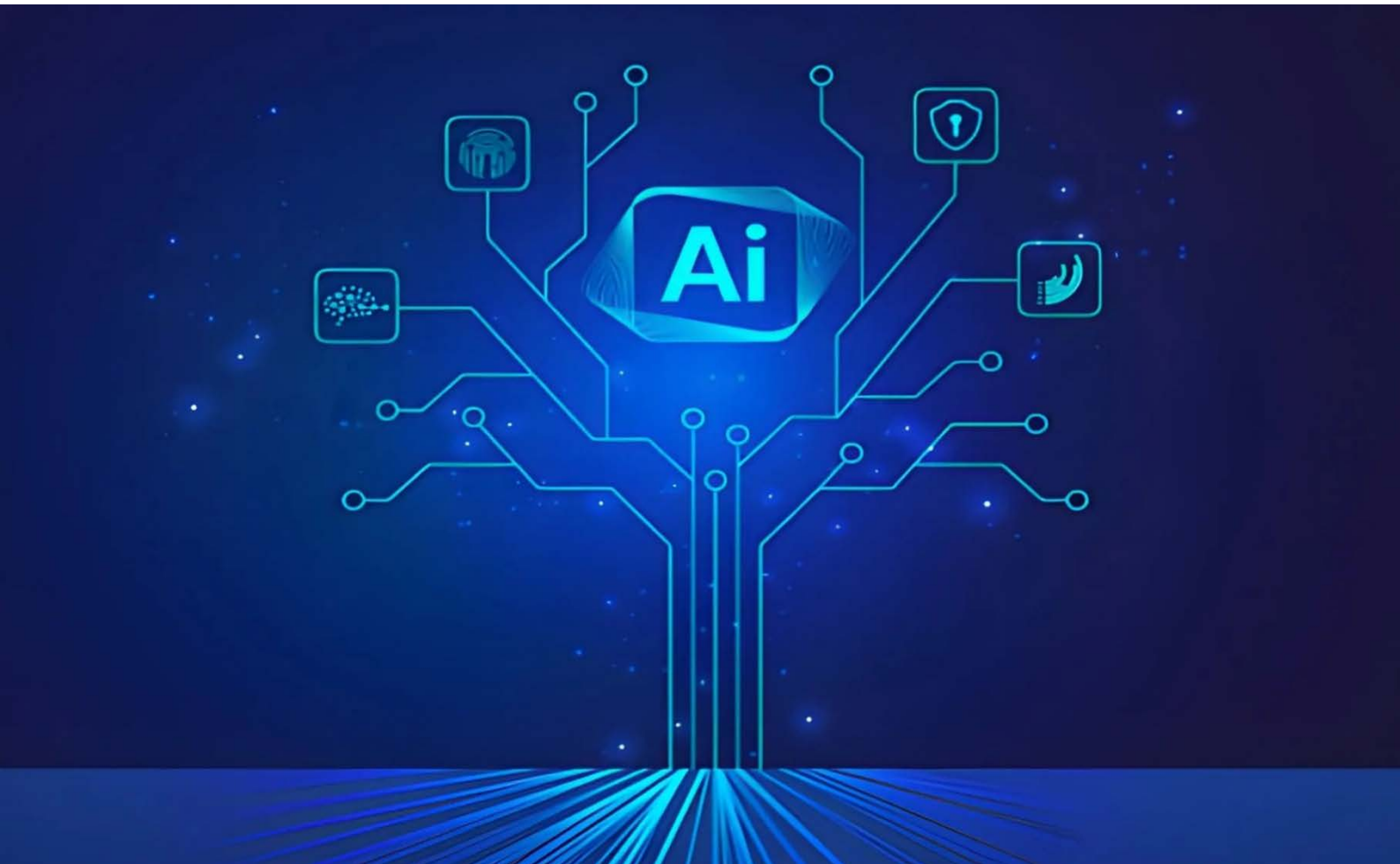
**END-TO-END RISK CONTROL**
The platform guarantees full traceability and continuous monitoring of models in production, reducing operational, regulatory, and reputational risks. AI risk is transformed from an unpredictable event to a manageable and measurable element.

**SCALABLE AND INDUSTRIALIZED AI**
By standardizing repositories, serving, and evaluation, models become reusable and governed assets, no longer isolated solutions.
This allows AI to scale sustainably, maintaining delivery speed and cost control.

**RELIABLE PERFORMANCE OVER TIME**
Active monitoring and user feedback allow us to detect drift, degradation, and bias in real time. Models continuously improve, ensuring stable performance aligned with business objectives.

**ALIGNMENT BETWEEN BUSINESS AND COMPLIANCE**
A single platform makes decisions, metrics, and accountability transparent throughout the model lifecycle. The result is more seamless collaboration between functions and faster, more informed decision-making.

**RESPONSIBLE INNOVATION AND RELIABILITY IN AI**
Integrated governance enables experimentation and adoption of advanced models (including generative ones) with complete security.
More control implies more trust, and more trust accelerates innovation.



# KEY VALUES

| | |
|---|---|
| *TRANSPARENCY* | Every model, data, and decision is traceable throughout the entire lifecycle, from training to production. This makes AI understandable, auditable, and governable even in complex contexts. |
| *CONTROL* | Deployment policies, continuous monitoring and rollback mechanisms ensure that models always operate within defined limits. The AI's behavior remains under control even in the presence of changes in the data or in the context. |
| *RELIABILITY* | Monitoring real-world performance and drift phenomena ensures stable results over time. The models maintain consistency with business objectives even in dynamic scenarios. |
| *RESPONSIBILITY* | Roles, ownership and decision-making processes are clearly defined and documented. Each choice is attributable, verifiable and aligned with corporate and regulatory policies. |
| *SUSTAINABILITY* | The platform enables continuous, secure, and sustainable evolution of AI solutions. |
| *FLEXIBILITY* | Ability to operate on-premise, in the cloud, or in hybrid infrastructures. |

**For more information:**
**cyberandsecurity@leonardo.com**

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



LDO_UK26_01877 04-26


leonardo.com