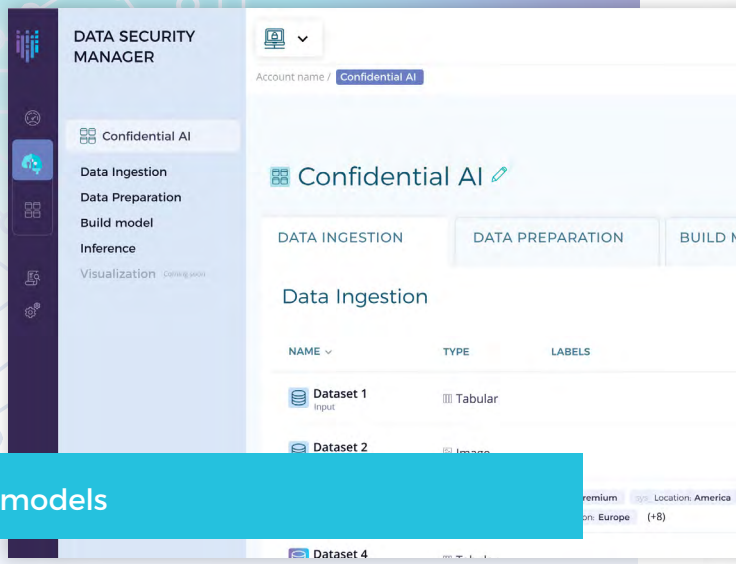
Fortanix®
CONFIDENTIAL AI

DATA SHEET



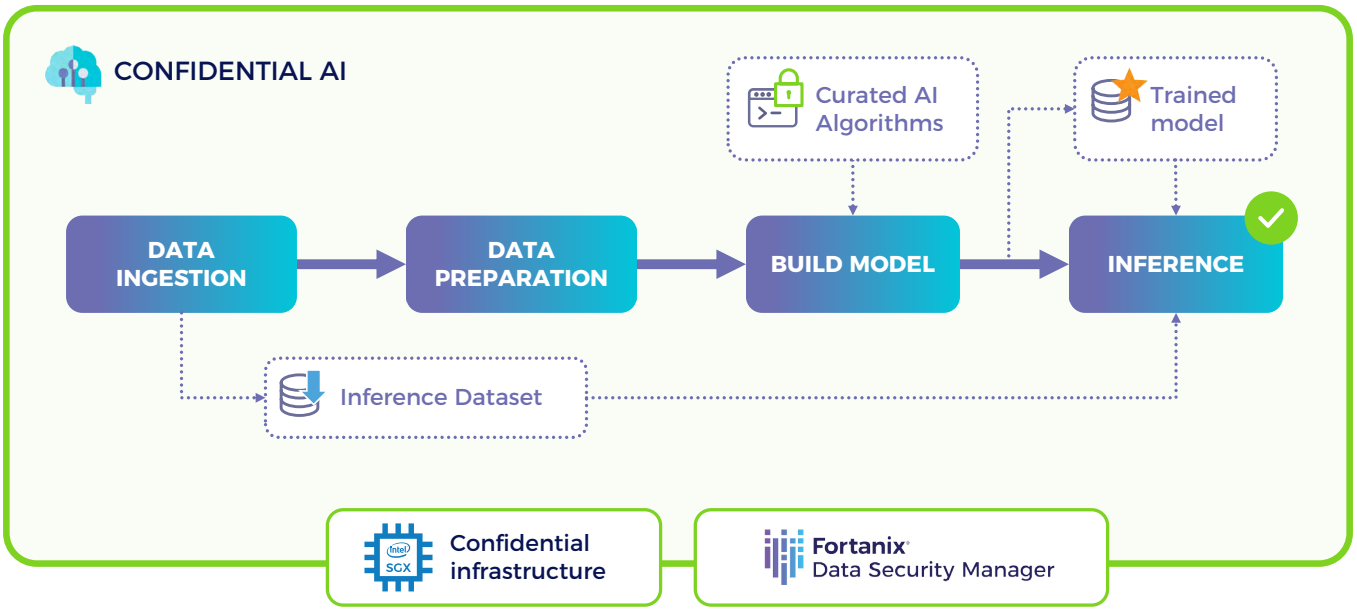
Fortanix Confidential AI

Unlock the power of private data and build smarter AI models

Fortanix Confidential AI is a service for developing and deploying AI models on sensitive data using confidential computing. The service provides multiple stages of the data pipeline for an AI project and secures each stage using confidential computing including DATA INGESTION, LEARNING, INFERENCE and model fine tuning. Fortanix Confidential AI is offered as an easy to use and deploy, software and infrastructure subscription service.

Unlike traditional AI solutions that focus on accelerating modeling processes, the Fortanix Confidential AI service provides data teams with -

- **MANAGED INFRASTRUCTURE** for model development and fine-tuning on sensitive data in a highly secure enclave
- generate **PREDICTIONS** by running data through pre-built or trained models, and
- proof of execution in a **TRUSTED EXECUTION ENVIRONMENT** with audit reports on processing and data provenance for compliance and data regulation.



Business Benefits

ALLEVIATE PRIVACY CONCERNS

With Confidential AI (C-AI), data teams get a secure environment to unlock the value of the most sensitive data while maintaining privacy and compliance. It alleviates concerns of exposing private data by running datasets in secure enclaves and provides proof of execution in a trusted execution environment for compliance purposes.

PROTECT INTELLECTUAL PROPERTY

Assures protection of the intellectual property of the models while providing access to richer private data for better quality and accuracy

NO-HASSLE DEPLOYMENT

The service is easy to deploy and provision with no technical expertise required.

The core capabilities of the platform include

- Managed confidential infrastructure running on Intel Ice Lake third generation scalable Xeon processors with Intel SGX support.
- AI models and frameworks enabled to run inside confidential compute.
- Dataset connectors to bring data from S3 accounts or upload of tabular data from local machines.
- Hardware backed proofs of execution of confidentiality and data provenance.
- Inference support for image data.
- Learning and inference support for tabular data.
- AI workflow orchestration via APIs and composable UI.

Supported Models

MODEL	FRAMEWORK	MODES	PROBLEM SUPPORTED	DATATYPE SUPPORTED
YOLOV5	PyTorch	Inference only	Object detection	Images
DECISION TREES	SciKit learn	Inference only	Classification Regression	Tabular
SVM (SUPPORT VECTOR MACHINES)	SciKit learn	Inference only	Classification Regression	Tabular
LINEAR REGRESSION	SciKit learn	Inference only	Regression	Tabular
KNN	SciKit learn	Inference only	Classification	Tabular and Images

Key Features

READILY AVAILABLE AND MANAGED CONFIDENTIAL INFRASTRUCTURE

Fortanix provides a readily available managed Confidential Computing infrastructure that's easy to deploy and provision.

DATA PREPARATION

Users can easily implement necessary data transformation using an ETL process running in a confidential computing enclave.

AUDITABLE REPORT AND LOGGING

Reports are provided for proof of execution in a confidential environment for all workflow executions. The report contains

- Curated application used for the processing
- Input Dataset used for the processing
- Output Dataset where the results were stored
- Infrastructure that the workload was run on.

DATA CONNECTOR

Dataset connectors allows for quick data ingestion. Bring from S3 accounts or upload data from local machines.

SUPPORT FOR FOUNDATIONAL AI ALGORITHMS

The solution supports a broad range of algorithms.

ONE-CLICK MODEL DEPLOYMENT

User can select a model to be used given their project objectives from a catalog of available models or upload a unique model to use in an encrypted and secure manner

ENTERPRISE GRADE SECURITY

Fortanix manages and enforces security policies including identity verification, data access control, and attestation to ensure the integrity and confidentiality of data, code, and applications.

INFERENCE SUPPORT

Inference support for image and tabular data.

CONFIDENTIAL INFRASTRUCTURE BASED ON NEXT GENERATION INTEL XEON PROCESSORS

Use of confidential computing in various stages ensures that the data can be processed, and models can be developed while keeping the data confidential even while in use. Implementations of well-known models to run inside SGX and other enclave technologies.

TRY OUT FOR FREE

Free trial of the service with all features enabled with four hours of compute time.

MODEL TRAINING

Select from a range of fundamental machine learning algorithms to train on datasets.

END TO END DATA PROTECTION

Integration with Fortanix Data Security Manager allows organizations to further enhance security through additional capabilities like key management and tokenization.

MONITORING

Track the status of production scenarios, success and failures using metrics and confidence scoring. User receives confirmation of success or failure from the job, including metrics from the model itself such as confidence scoring, and an auditable report including Confidential Computing attestations, which data sets were used and what keys were used.

MODERN SCALABLE ARCHITECTURE

Fortanix managed and deployed infrastructure works on the scalable architecture powered on Azure AKS with SGX enabled nodes.

PAY FOR COMPUTE THAT YOU USE

Usage based billing after the free trial period ends, charged monthly basis.

How can I take the next step?

1. Visit our Confidential AI web page at https://fortanix.com/products/confidential-AI/
2. Take a free assessment – Fill up the form and talk to Fortanix experts for a free assessment of your AI project infrastructure
3. Try the service for free

Support services

Fortanix Technical Support is included in SaaS Subscription licenses for Confidential-AI. Fortanix support is designed for enterprises that operate Fortanix products in a mission-critical 24x7 environment and cannot afford any downtime. For severe issues, support services are available 24 hours a day, 7 days a week.

24X7 TELEPHONE, EMAIL, AND WEB SUPPORT:
Fortanix support engineers will answer technical questions and assist with data security operations 24 hours a day.

ACCESS TO EXPERTS THROUGH OUR SLACK COMMUNITY.

PRIORITY CALL-HANDLING:
Customer calls are given priority status and handled by the next available support engineer.

TALK TO OUR EXPERTS FOR A FREE ASSESSMENT OF YOUR AI PROJECT INFRASTRUCTURE

TAKE A FREE ASSESSMENT NOW!