truefoundry

TrueFoundry Platform Security

The TrueFoundry platform provides maximum security with complete customer isolation

TrueFoundry is trusted by our customers for across the board ML and LLM requirements. This document provides an overview of the TrueFoundry platform architecture, compliance and platform security features that enable your teams to deploy securely, enforce authorization, and protect your data.

NOTE: This document assumes at least the Enterprise-tier TrueFoundry subscription. TrueFoundry can be installed on AWS, GCP, Azure and on-prem clusters.

Architecture

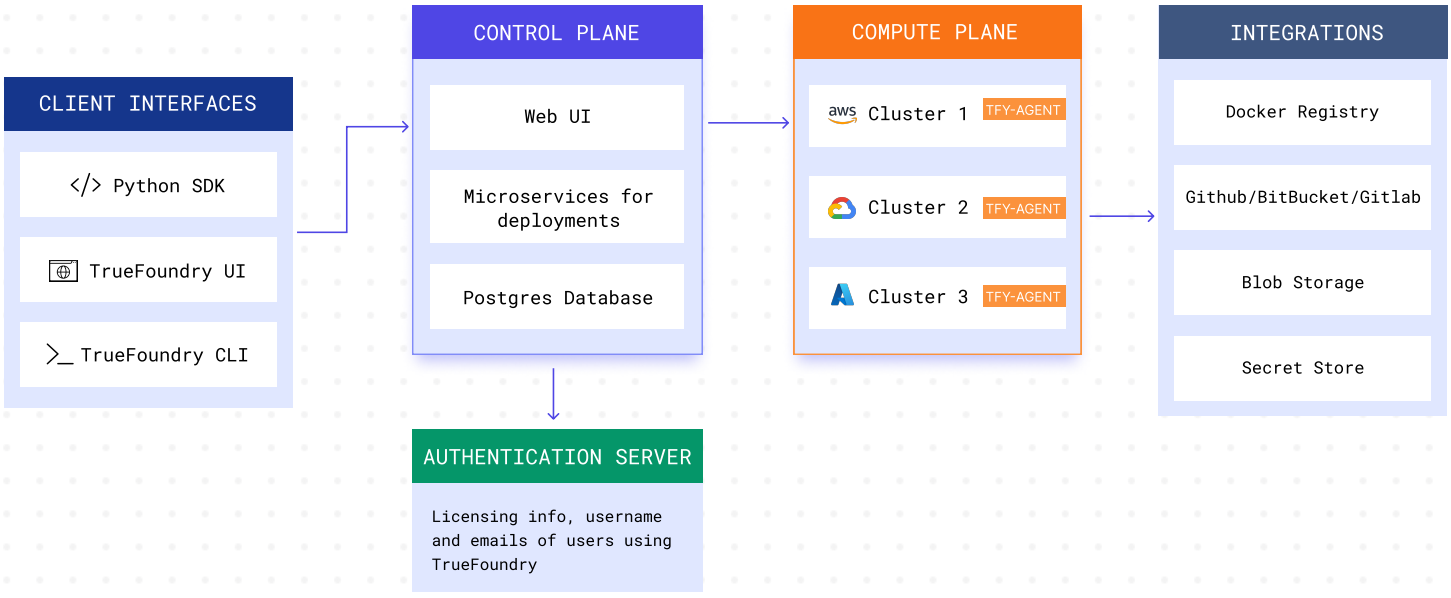
It comprises of 4 main components:

1. **Control Plane**: This is the brain of the TrueFoundry system which does the orchestration of deployments across the different compute plane. For enterprise customers, the control plane is deployed on the customers' cloud. It comprises of UI, multiple microservices which orchestrate the deployments, and a Postgres database.

2. **Compute Plane**: This is the Kubernetes cluster on which the user's code runs. There is an agent on the compute plane (tfy-agent) which communicates with the control plane and executes the commands received from the control plane. The user's code accessing the data runs on the compute plane - and hence the compute plane cluster should live close to data.

3. **Client Interfaces**: Developers and data scientists can communicate with the UI using a python SDK, our web UI or using the TrueFoundry CLIs (servicefoundry and mlfoundry).

4. **Authentication Server**: There is a central authentication and licensing server that keeps track of all the organizations and their members. This server is hosted by TrueFoundry and can also integrate with external IDPs to provide a single sign-on experience to all our users. It stores tenant name, username and emails of the users registered on TrueFoundry that could be part of your development/ML/infra/other teams.



How is TrueFoundry deployed?

For enterprise plan, we do a private deployment. This means both the control plane and the compute plane resides on your private cloud account.

What is deployed on your cloud accounts?

1. The control plane is shipped and deployed on your choice of cloud account. We support AWS, GCP, Azure and on-prem setup.

2. A new cluster is created and connected to TrueFoundry. This is called the compute-plane cluster. It is where we install tfy-agent and other add-ons to enable full functionality of the platform like logs, monitoring, job deployment etc.

What remains with us?

Authentication server will remain as part of TrueFoundry. This is a central authentication and licensing server that keeps track of all the organizations and their users. It stores tenant name, username and emails of the users registered on TrueFoundry that are part of your development/ML/infra/other teams. This server is hosted by TrueFoundry and can also integrate with external IDPs to provide a single sign-on experience to all the users.

Network and server security

Below, we'll review networking, servers and how TrueFoundry interacts with your cloud service provider account

Networking

In TF setup all the workload is deployed completely on user's own cloud account. This basically means that any and all networking policies specific to the customer's own requirement can be implemented.

TrueFoundry does not rewrite or change your data structure in your storage, nor does it change or modify any of your security and governance policies.

TrueFoundry also offers a networking setup such that connections only from VPN or official IPs are allowed.

Servers

In the compute plane, TrueFoundry automatically run the latest hardened system image. Users cannot choose older (less secure) images or code.

TrueFoundry code is peer reviewed by developers with security training. Significant design documents go through comprehensive security reviews. Scans run fully authenticated, with all checks enabled.

TrueFoundry access

As both control plane and compute plane are deployed on the customer's cloud, we will not have access to any of the systems or data except the tenant name, username and emails of the users using TrueFoundry platform that are part of your teams.

Data and cloud security

TrueFoundry provides maximum security with complete customer isolation by doing a private deployment on the customer's cloud. TrueFoundry leverages the native physical and network security features of the cloud service, and relies on the providers to maintain the infrastructure, services, and physical access policies and procedures.

Encryption

Client's data protection complies with SOC 2 standards to encrypt data in transit and at rest, ensuring customer and company data and sensitive information is protected at all times.

1. All the data at rest is encrypted which includes the Postgres DB and all the persistent volumes which are part of control plane.
2. Customers can use encrypted storage buckets.
3. Every connection between control plane to compute plane is TLS encrypted.

Role Based Access Control

Customers can isolate users and data at both account level and resource level:

1. Account level: Create super admins with access to everything or member who gain access to resources only when invited.
2. Cluster level: Restrict which users can manage clusters and workspaces.
3. Workspace level: Restrict which users can manage workspace and deployments.
4. ML Repo level: ML Repos are our resources which connect to S3 buckets. You can store models, artifacts and other data using ML Repo. You can add RBAC for each ML Repo to isolate data between teams and users.

Activity Logs

Activities of TrueFoundry users are logged and can be delivered automatically to a cloud storage bucket.

Compliance

TrueFoundry is committed to providing secure products and services to safely and easily manage billions of digital identities across the globe.

Our external certifications provide independent assurance of TrueFoundry's dedication to protecting our customers by regularly assessing and validating the protections and effective security practices TrueFoundry has in place.

Currently, TrueFoundry is SOC2 Type 2 and HIPAA compliant.

Secure Personnel

TrueFoundry takes the security of its data and that of its clients and customers seriously and ensures that only vetted personnel are given access to their resources.

- Confidentiality or other types of Non-Disclosure Agreements (NDAs) are signed by all employees, contractors, and others who have a need to access sensitive or internal information.
- We embed the culture of security into our business by conducting employee security training & testing using current and emerging techniques and attack vectors.

Secure Development

- All development projects at TrueFoundry, including on-premises software products, support services, and our own cloud offerings follow secure development lifecycle principles.
- All development of new products, tools, and services, and major changes to existing ones, undergo a design review to ensure security requirements are incorporated into proposed development.
- All team members that are regularly involved in any system development undergo annual secure development training in coding or scripting languages that they work with as well as any other relevant training.

Secure Testing

TrueFoundry deploys third party penetration testing and vulnerability scanning of all production and Internet facing systems on a periodic basis.

- All new systems and services are reviewed and tested prior to being deployed to production.
- We perform penetration testing by external penetration testing companies on the entire product on a periodic basis to ensure a comprehensive and real-world view of our products & environment from multiple perspectives.
- We perform vulnerability testing of all code, including open source libraries, as part of our software development process.

Learn more

For more information, connect with us. TrueFoundry provides an enterprise-ready cloud platform that is built on a strong platform security posture for organizations small and large, and across all industries.

We're happy to discuss your specific needs in more detail — please reach out to us on support@truefoundry.com.

About TrueFoundry

Train and deploy ML models and LLMs on top of Kubernetes at the speed of Big Tech with 100% reliability and scalability. Slash production costs by 30-40% and release models to production faster. Run training jobs, inference services, GPUs and more on your own infra. To learn more, follow TrueFoundry on Twitter, and LinkedIn.