Secure Deployment Options

Abacus.AI Platform

Abacus.AI is an AI-assisted Data Science & MLOps platform to help enterprises develop and operate sophisticated machine learning models across a variety of enterprise use-cases such as personalization using recommendation engines, forecasting, and anomaly detection. For a comprehensive description of our product offerings please refer to https://Abacus.AI.

Abacus.AI has implemented comprehensive security controls across every aspect of the product development, engineering, operational processes, hosting, and delivery life cycles. These security controls were developed and implemented with the singular goal of safeguarding our customer's data using best-in-class industry frameworks and practises. For a comprehensive description of our security posture please refer to https://Abacus.AI/security.

Secure Deployment Options

- Option 1 : Multi-tenant SaaS on AWS, GCP, or Azure
- Option 2 : Single-tenant VPC; owned and operated by Abacus
- Option 3: Customer owned Storage Location (AWS/GCP/Azure)
- Option 4 : Customer owned VPC; operated by Abacus (*need control-plane access from Abacus*)

Common security features (*all options*)

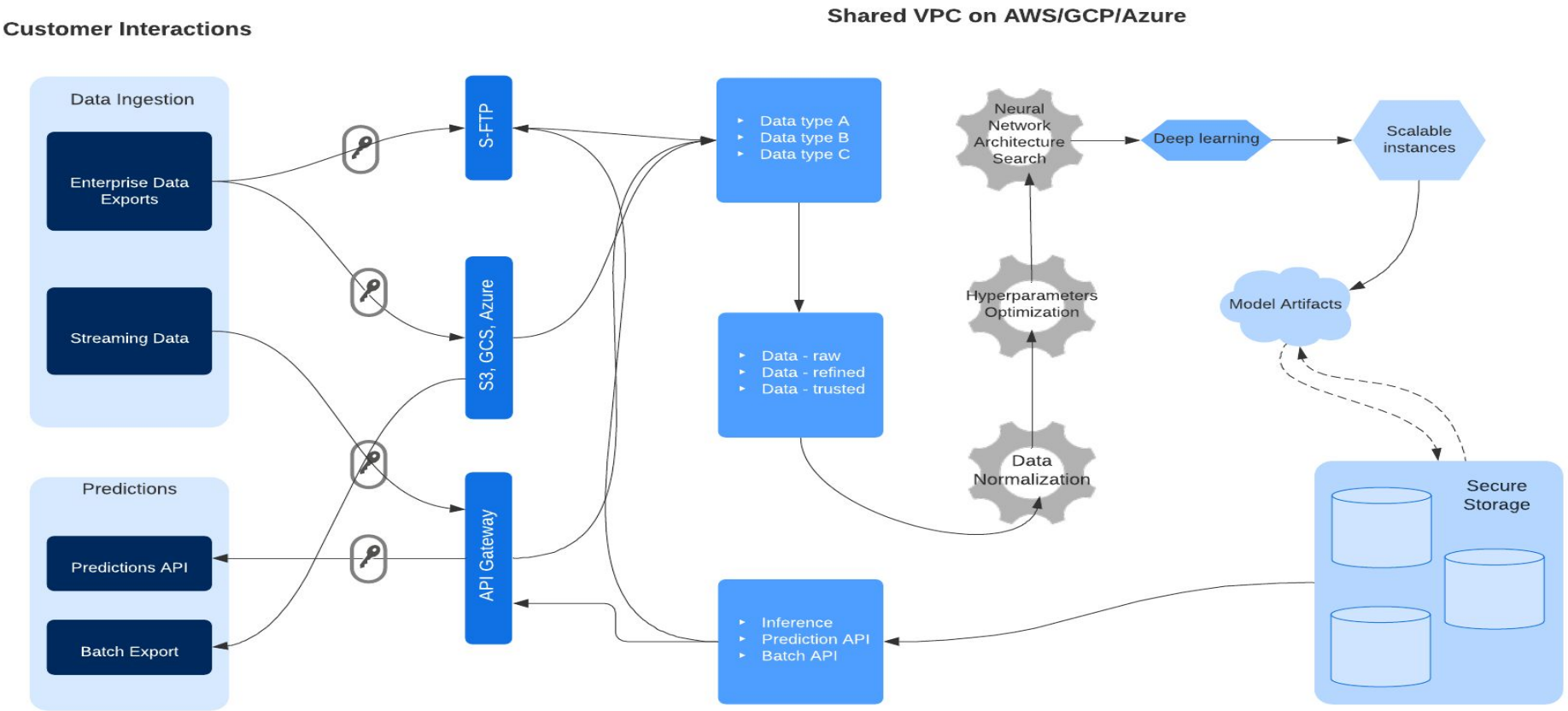
All deployment options come with the following security features:

- All data encrypted at rest and transit
- All data encrypted with dedicated customer encryption keys
- All compute isolated in dedicated ephemeral job processing pipelines
- Compliance with all applicable local regulatory and standards compliance (SOC2 Type 2, HIPAA, CCPA, GDPR, CIS, PCI DSS)

Option 1: Multi-tenant SaaS (*AWS, GCP, Azure*)

- Hosted on Public Cloud (*Aws*, *Gcp*, *Azure*) of customer's choice
- Storage & Compute isolation
- Network isolation based on TLS
- Least amount of setup time
- Zero requirements from customer infrastructure and operations teams
- Static Egress IPs, VPC network peering available

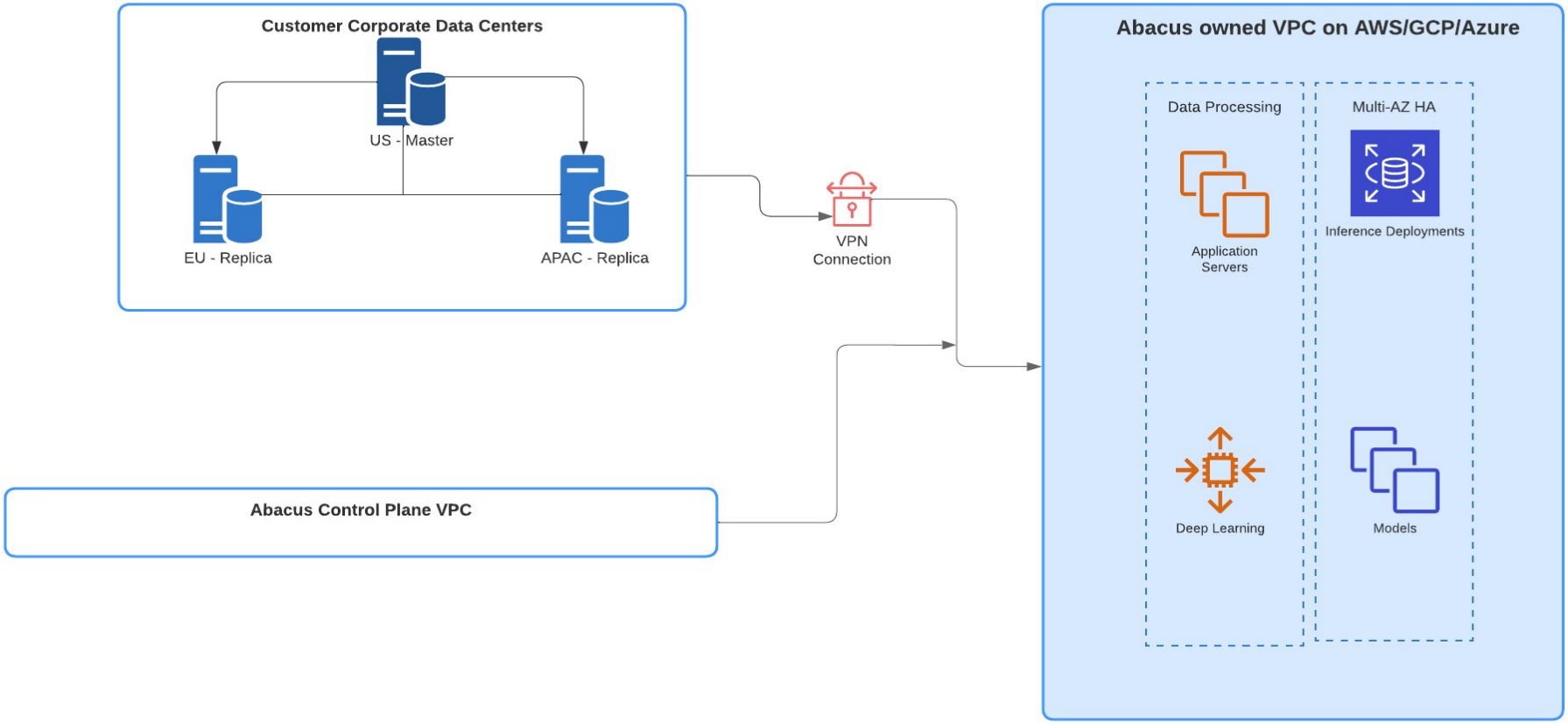
Option 1 : Multi-tenant SaaS



Option 2: Single-tenant VPC; owned/operated by Abacus

- Abacus sets up a dedicated single tenant VPC per customer
- VPC can be setup in any of AWS, GCP, Azure cloud environments
- Abacus will own and operate the vpc environment; including infrastructure setup and costs

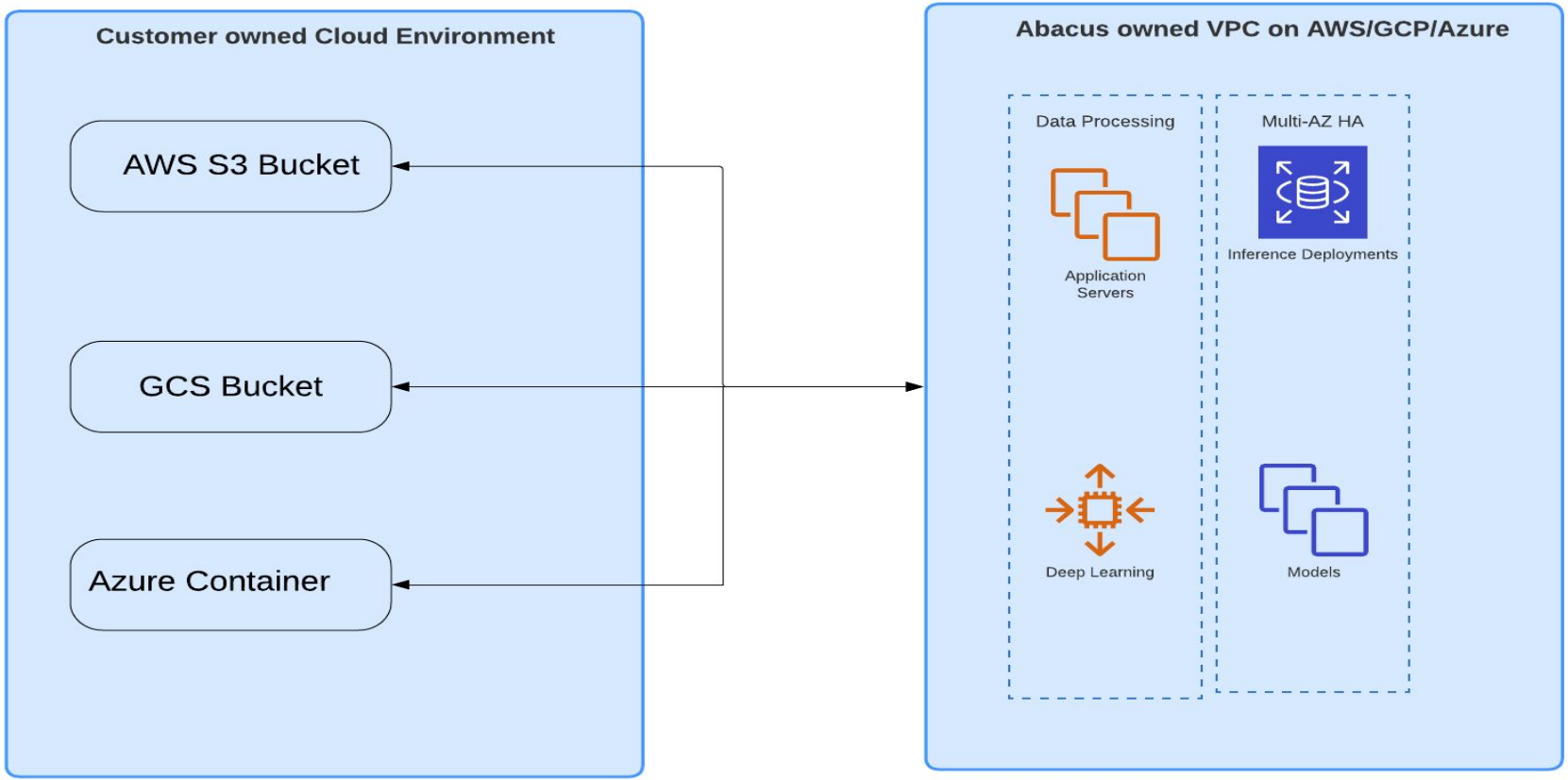
Option 2 : Single tenant VPC; owned, operated by Abacus



Option 3: Customer owned storage location

- This is a variation of either Option 1 or Option 2
- Customer owned storage location:
  - AWS S3 bucket
  - Google Storage Bucket
  - Azure Storage Container
- Abacus will use that location for all model artifacts, vector store indexes, materialized feature groups etc.
- Security boundaries:
  - AWS VPC Peering
  - Google Service Controls (limit access from some Project IDs)
  - Azure Private networking

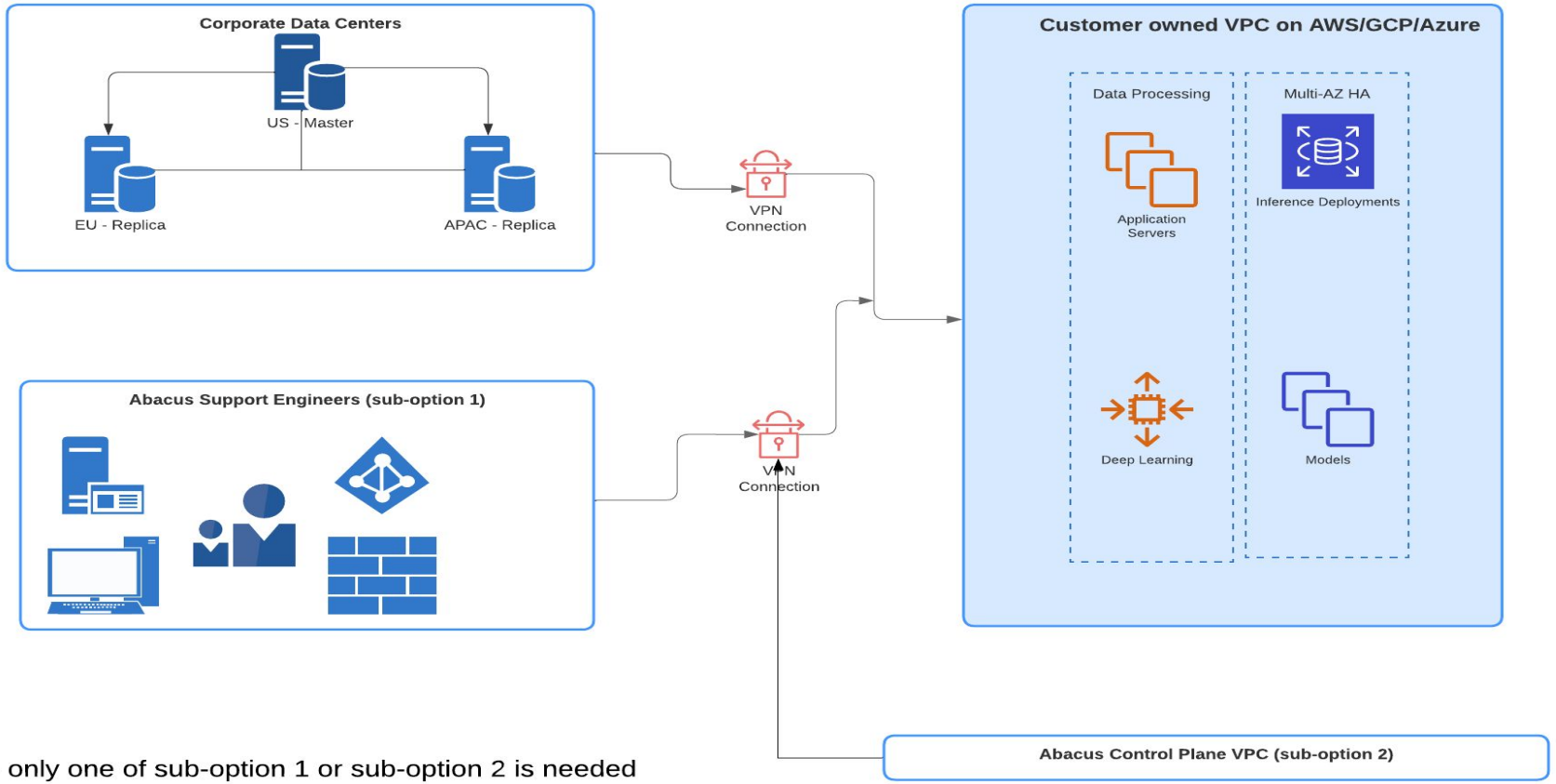
Option 3 : Customer Owned Storage



Option 4 : Customer owned VPC; operated by Abacus

- Customer's infrastructure team sets up a VPC in AWS/GCP/Azure public cloud environments
- Requirements:
  - Kubernetes cluster with dedicated namespace "abacus" (EKS/GKE/AKS is ok)
  - Cloud Object storage (AWS s3 bucket, Google GCS bucket, Azure container)
  - Container registry (with access to Abacus to push docker images to)
  - Abacus control plane access (inbound to kubernetes api server, load balancer)
  - OR
  - Consultant laptop, vpn access for 2 Abacus engineers

Option 4 : Customer owned VPC; operated by Abacus



Note - only one of sub-option 1 or sub-option 2 is needed