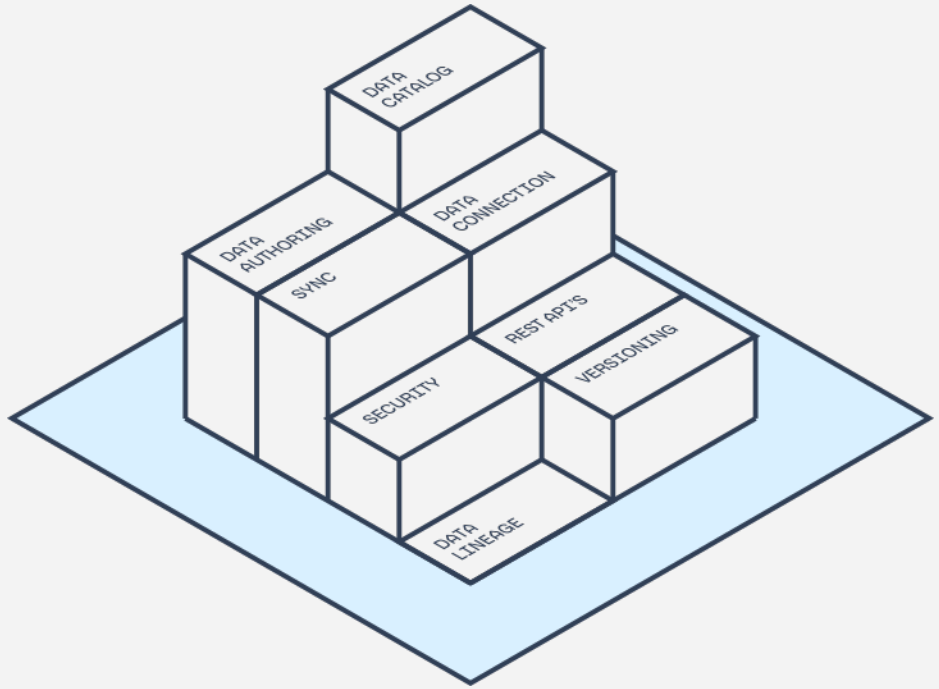
Foundry Technical Onboarding



Palantir FOUNDRY

Intro to Palantir

Palantir enables organizations to solve their hardest problems using data.

Headquarters	Founded	Employees	Offices worldwide
Denver, CO	2004	2,400	20+

SOME OF OUR PARTNERS

MERCK · SANOFI · NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN TEXAS REGIONAL OFFICE · CREDIT SUISSE · Ferrari · AIRBUS · WFP · U.S. DEPARTMENT OF DEFENSE · ANHEUSER-BUSCH · Swiss Re

INDUSTRIES WE WORK WITH

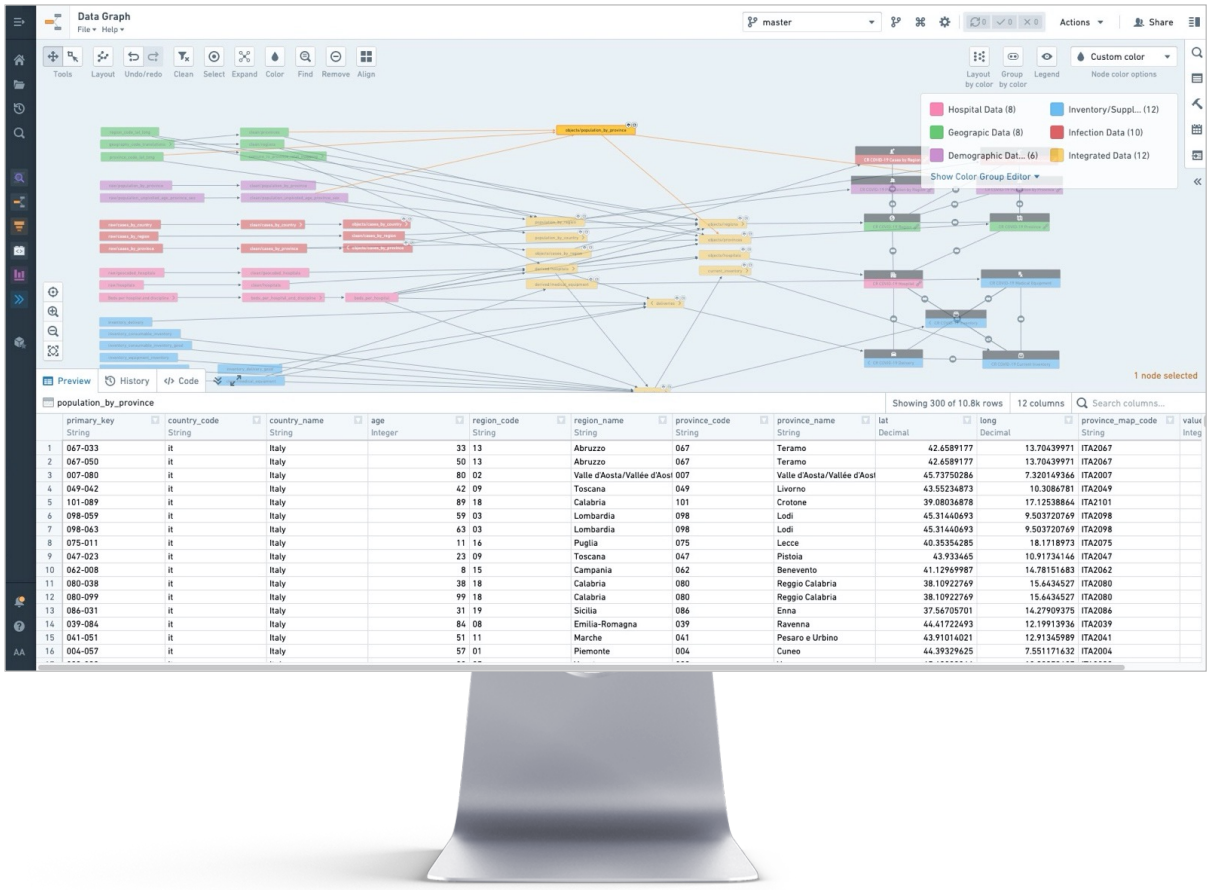
Defense	Energy	Media
Intelligence	Law Enforcement	Automotive
Disaster Response	Aviation	Humanitarian Aid
Manufacturing	Healthcare	Telecom
Finance	Regulatory	Cybersecurity
Shipping	Logistics	Insurance
Pharma	CPG	Tech

Palantir FOUNDRY

Foundry is Palantir’s managed SaaS for deriving decisions from data

Foundry unifies organizations around their central mission, enabling them to become fully digital “connected organizations”:

- → Integrated data operations
- → Git-style branching & collaboration
- → Full data & logic lineage
- → Automatic propagating security & governance
- → Operational application suite of tools



Palantir FOUNDRY

Foundry is Palantir’s managed SaaS

Foundry includes industry-standard and advanced backing platform features.

Autoscaling Infrastructure

Foundry incorporates an autoscaling infrastructure that scales based on your immediate compute needs

Managed SaaS

Palantir Cloud Operations Infrastructure alerting, monitoring & support to ensure performance

Microservice Architecture

Modular software development without user downtime or broader impact

24/7/365 Monitoring & Support

Palantir Cloud Operations Monitoring & Support

Continuous Delivery & Automated Upgrades

Rapid online upgrades and patching without system-wide effects

High Availability & Disaster Recovery

Designed and deployed with High-Availability & Disaster Recovery in the case of critical failures

Encryption in-transit & at rest

Data, applications, and communications are encrypted throughout Foundry

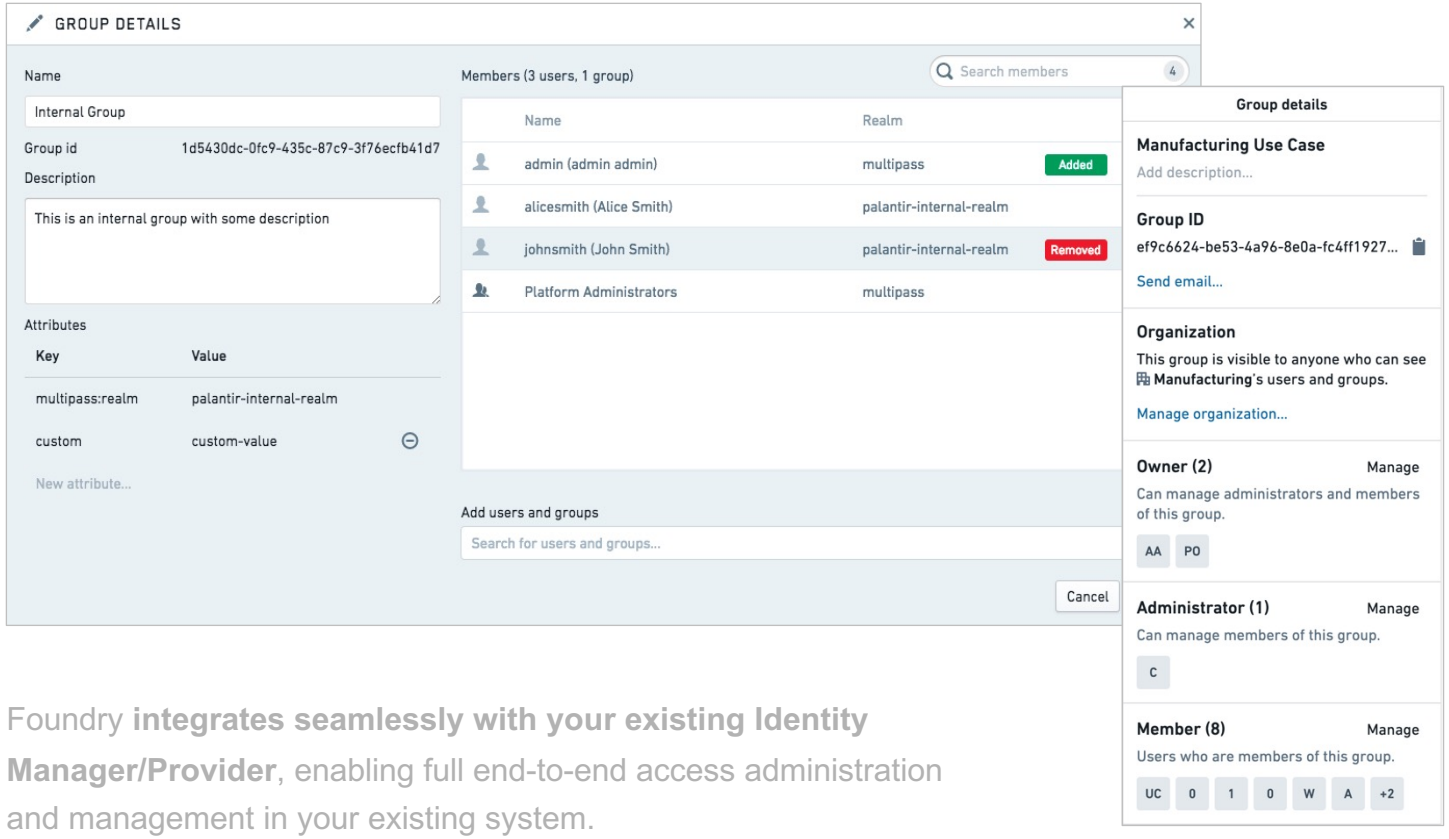
Single-Sign On and Access Control

Control access into & within Foundry through existing Single Sign-On identity providers

Foundry gives customers best-in-class security controls

Foundry has a robust set of operational security primitives natively built into the platform, giving you the necessary tools to enforce proper control over your data.

- → Permission by users and nest-able groups
- → Role-based access controls
- → Propagating security model
- → Granular Permissions / Row-level Security
- → Admin Permissions View



Foundry **integrates seamlessly with your existing Identity Manager/Provider**, enabling full end-to-end access administration and management in your existing system.

Palantir FOUNDRY

Foundry’s environment is secured and monitored

Foundry operates with a robust security-focused infrastructure, leveraging state-of-the-art security practices and protocols

Encryption in transit and at rest

- → Communication between services occurs over TLS 1.2+, only encrypted HTTPS endpoints are exposed and strict Ingress/Egress rules are enforced for the platform
- → All storage layers, including object stores, block storage, and disk volumes, are secured with server-side encryption

Vulnerability management

- → Palantir’s Information Security team performs continuous internal penetration testing and security reviews, as well annual third-party penetration tests that cover white, gray, and black box testing of user interfaces and back-end APIs

Audit logs

- → Application audit logs can be made available for the customer to ingest into their existing SIEM for further analysis and monitoring of user actions within Foundry

Certifications and Attestations

Palantir maintains rigorous, externally verified infrastructure and operations standards.

Foundry is **externally certified** for the following baselines:

1. SOC 2 Type II
2. ISO 27001, ISO 27017 and 27018
3. FedRAMP Moderate (Foundry for US Government)
4. US DoD Impact Level 5 (Foundry for US DoD)

On top of those certifications, we are **aligned** with the controls and policies of:

1. NIST 800-53 and 800-171
2. ISO 27002, 27003
3. ISO Business Continuity and Risk Management Standards

In addition, Palantir has extensive experience helping customers meet specific **regulatory and industry requirements**, including:

1. EU General Data Protection Regulation (**GDPR**)
2. US Health Insurance Portability and Accountability Act (**HIPAA**)
3. California Consumer Privacy Act (**CCPA**)
4. Federal Information Security Modernization Act (**FISMA**)

Sign-up steps

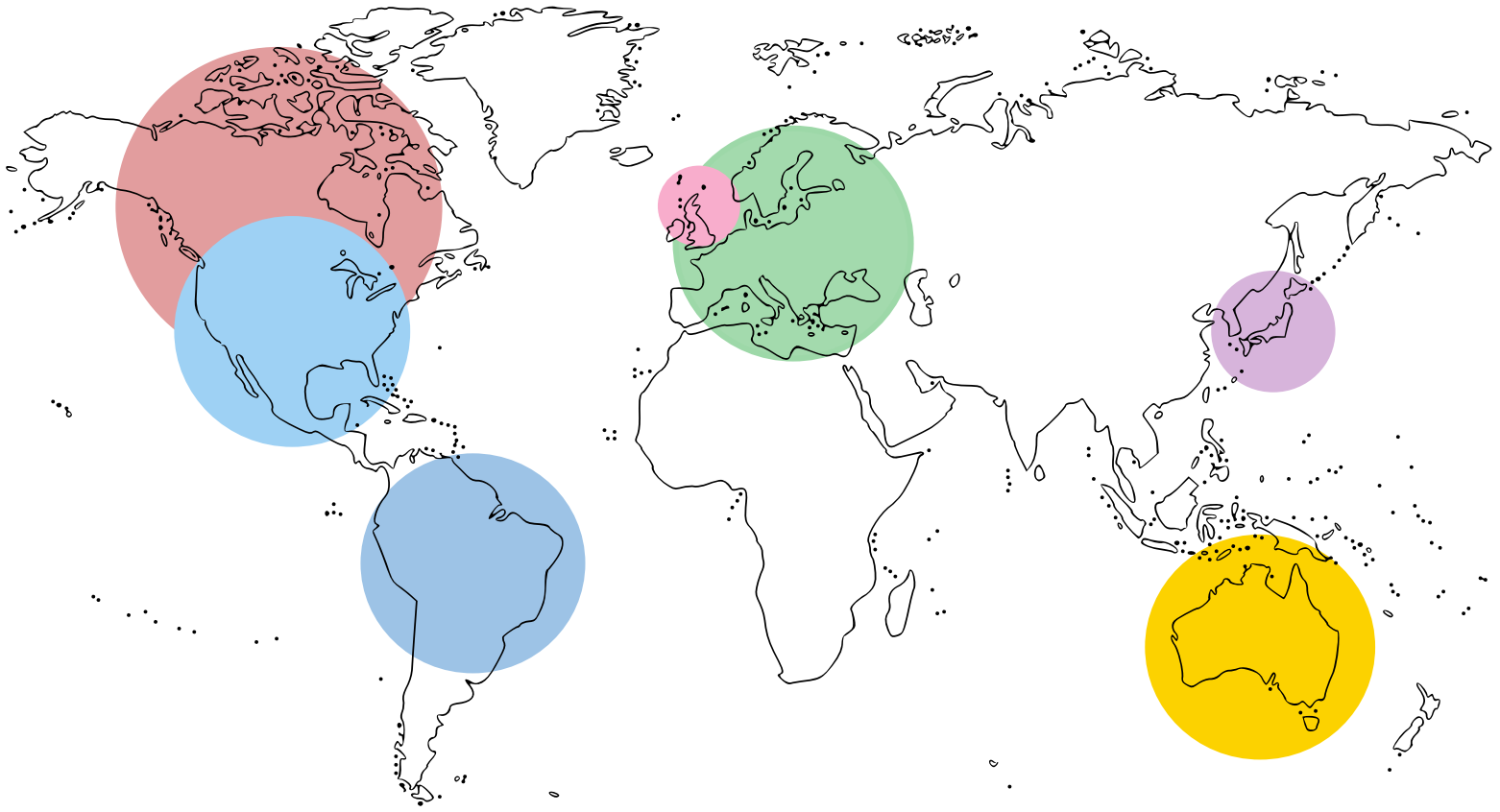
There are six steps to complete in signing up to Foundry.

1. Select your region	Choose the region for your Foundry.
2. Select your domain	Palantir can either generate a domain for you, or we can have Foundry accessible through a subdomain with your chosen customer domain.
3. Configure the Data Connector	Configure either the on-premise or cloud Data Connector to connect Foundry to your sources.
4. Set-up Single-Sign On	Confirm attributes and send your organization's SSO identity provider metadata for easy access to Foundry from your existing SAML system.
5. Share your users' country locations	This is for us to ensure that they can access Foundry.
6. Review our standard security assessments	Upon request, we will provide comprehensive documentation required for standard security reviews.

1. Select your region

Available regions for your Foundry's data residency:

- → United States
- → Canada
- → European Union
- → United Kingdom
- → Japan
- → Australia
- → Brazil



2. Select your domain

There are two possible options for your Foundry domain.

1. [Recommended] Customer-defined with Palantir domain

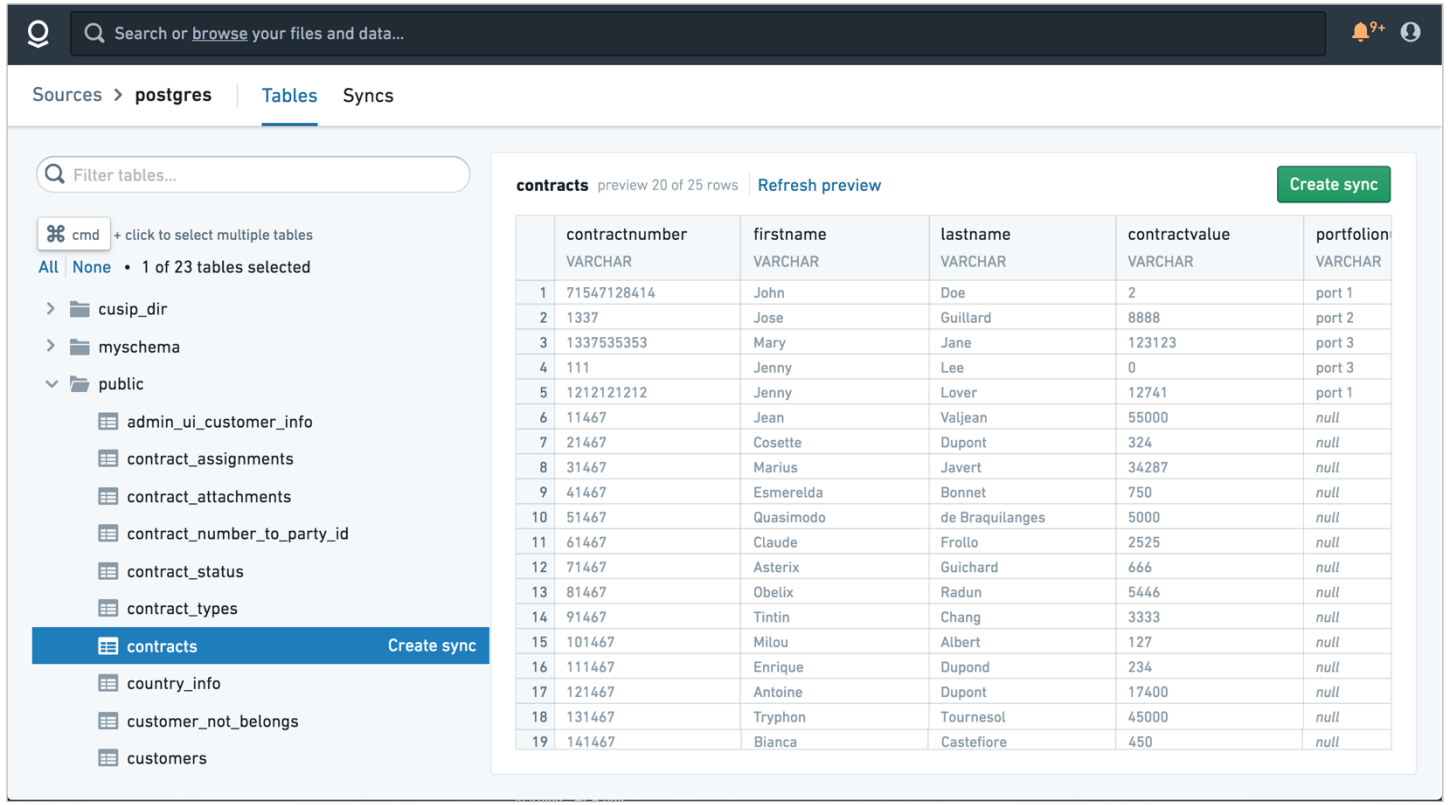
- → You choose a subdomain, and Palantir creates a unique domain for you with that subdomain, such as **`https://<subdomain>.palantirfoundry.com.`**
- → The subdomain can be the name or acronym for your organization, or any codename you choose. Some customers prefer to choose a codename to avoid putting their name in public DNS records.

2. Customer-generated domain

- → *Warning: this option can be slower to set up, and may delay getting access to your Foundry environment.*
- → You choose a subdomain within your own organization's domain, such as **`https://foundry.<customer>.com`**, and set up a C-NAME to the alias for your selected Foundry region.
- → Palantir generates a certificate signing request (CSR), which we will send to you to be signed by the Certificate Authority used by your organization.

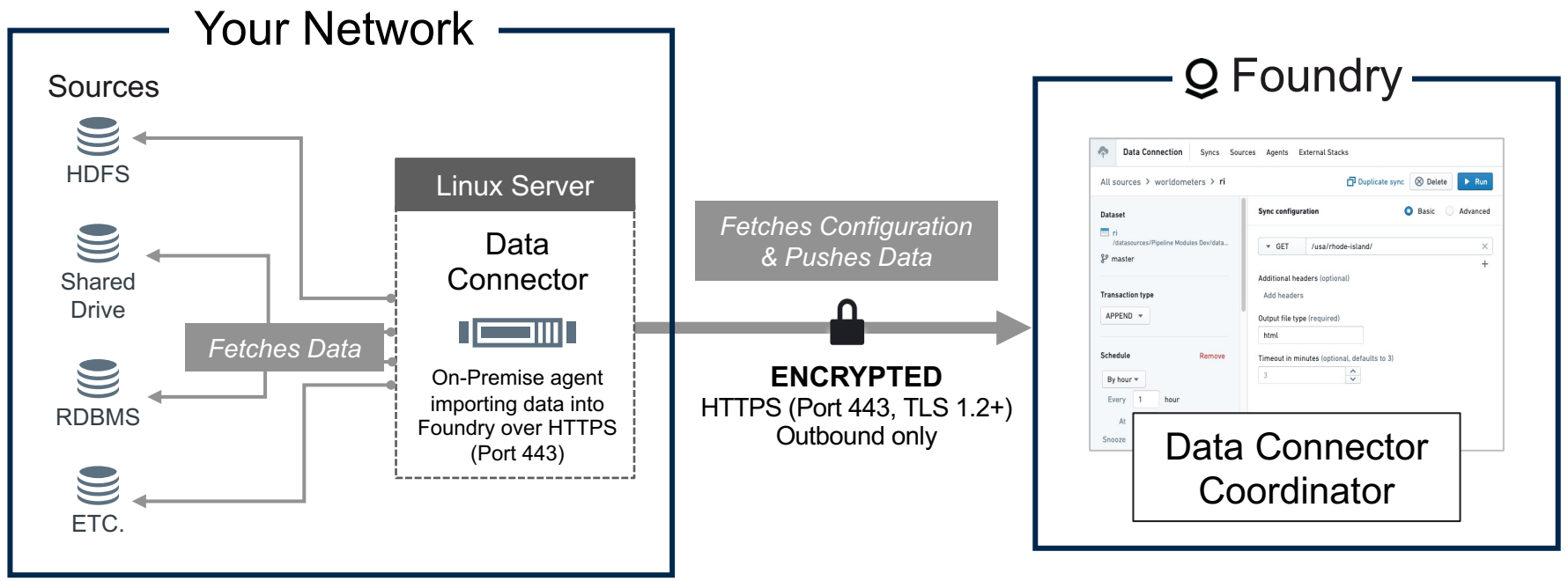
3. Configure the Data Connector

- Users schedule and execute data syncs through an intuitive and access-controlled UI
- Depending on the location of your sources, we have an **On-Premise Data Connector** we can deploy and a **Cloud-based Data Connector** for your cloud-based source systems



3. Configure the Data Connector | Option A: On-premise Data Connector

- The cloud-based Coordinator configures and executes jobs that tell the Data Connector how to migrate new data
- The Data Connector communicates with your on-premise sources to fetch data
- The on-premise connector communicates with the Coordinator via encrypted outbound-only HTTPS requests.



3. Configure the Data Connector | Option A: On-premise Data Connector

Common points of contact for on-premise installation:

Networking/Infrastructure

- → Provisions server for Data Connection in appropriate location, as well as remote access
- → Allowlist the Foundry IP addresses to the provisioned server

Data Source Owners

- → Help identify data source for ingestion, as well as supporting materials such as data dictionaries
- → Obtain any required approvals for data and/or source system access

Customer server provision — Provision a server for the Data Connector with appropriate user accounts created and at least the following specs:

- → [4 Physical Cores] - [16 GB RAM] - [500 GB Hard disk] - [64-bit Unix-based operating system]

Palantir provides IPs — Palantir will provide the qualified domain name and IP addresses for Foundry

Customer allowlist — Customer will allowlist the Foundry IPs in order to allow outbound connections from the server to Foundry

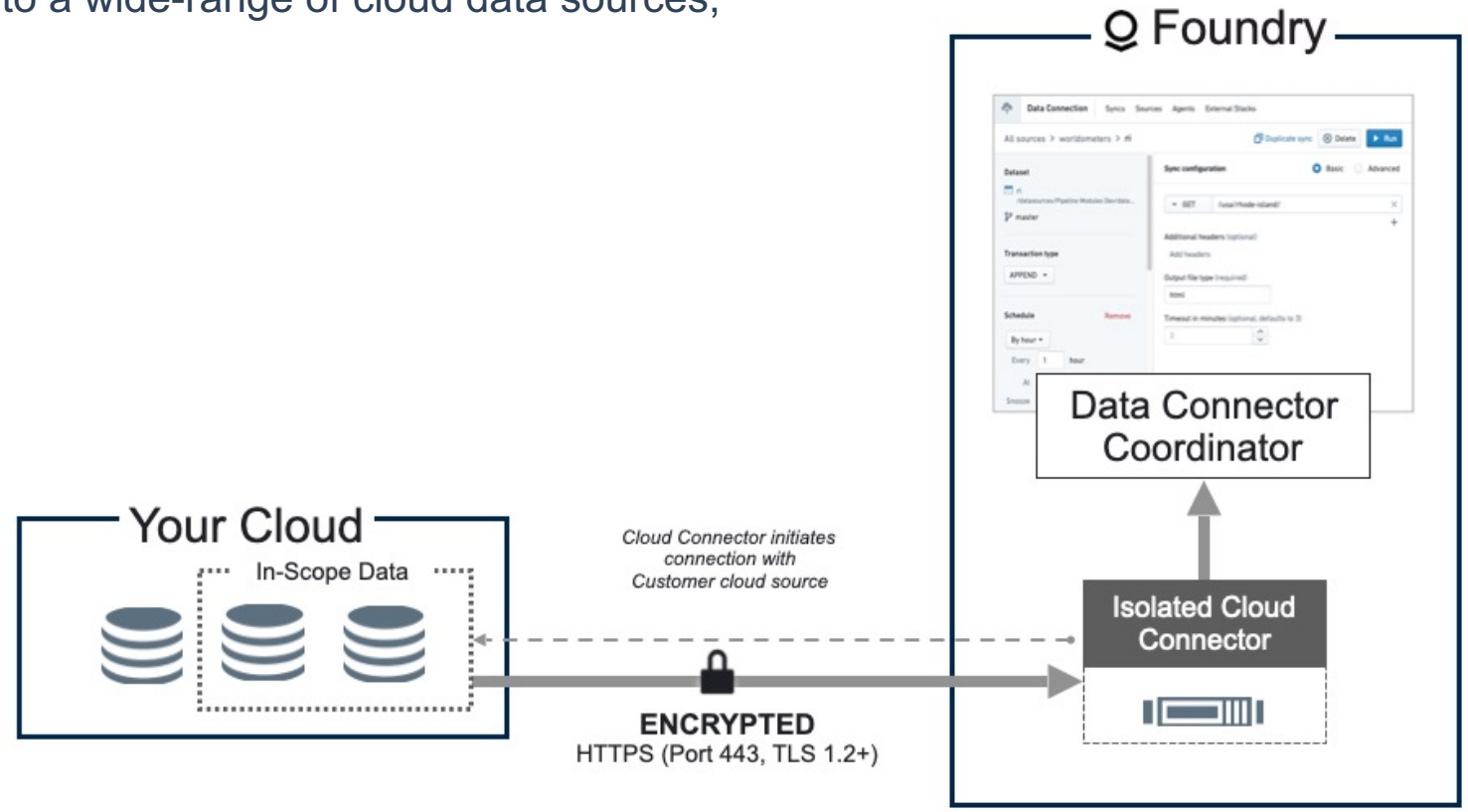
Customer source networking access — Customer will enable open connections between the Data Connector server and relevant Source Systems

Customer source connection information — Customer will share configuration options (e.g. private IPs, ports, credentials) for the Data Connector to source system connection

3. Configure the Data Connector | Option B: Cloud-based Data Connector

The cloud-based cloud connector can connect to a wide-range of cloud data sources, including:

- → Amazon S3
- → AWS Redshift
- → Azure Data Lake Storage
- → Azure Blob Storage
- → Box Drive
- → Google BigQuery
- → Google Cloud Storage
- → Oracle File Storage
- → Salesforce



4. Set-up Single Sign-On

Foundry easily integrates with your existing Single Sign-On provider.

Foundry has a native **Multi-Factor Authentication** service, so if MFA is not enabled at your organization, we can enable this service for an additional level of protection.

Foundry supports any **SAML 2.0** identity provider (IdP), including the following:

- → Azure AD
- → ADFS
- → Okta
- → PingFederate
- → Shibboleth
- → KeyCloak
- → Hennge One
- → GEOAxIS
- → DISA GCDS

5. Share your users' country locations

Please let us know your users' country for us to ensure that they can access the platform.

Summary of Sign-up steps

1. Select your region

[United States] - [Canada] - [European Union] - [United Kingdom] - [Japan] - [Australia] - [Brazil]

2. Select your domain

→ Selecting a custom subdomain within a Palantir domain

→ Utilizing a Palantir randomly-generated domain

3. Configure the Data Connector

Depending on the sources, pursue an on-premise option or cloud option for data connection:

On-premise

→ Customer provisions the Linux Server

→ Customer allowlists Palantir-provided Foundry IPs

→ Customer shares source system configuration

→ Palantir and customer perform installation

Cloud

→ Customer shares source system configuration

4. Configure Single Sign-On

Confirm the use of MFA in your SSO and:

→ Generate the appropriate SAML IdP metadata

→ Confirm the SAML attributes that will be passed

→ Upload SP metadata to your SSO once provided by Palantir

5. Share your users' country locations

We will allowlist access to Foundry to the IPs from these countries.

6. Fulfill any security assessments or SaaS vendor evaluation forms

We can respond to any questionnaires your organization requires to host data in the Foundry environment.