Coiled Security Overview

About Coiled

Coiled is a SaaS platform for orchestrating scalable Python workloads using Dask directly within a customer's AWS environment. It empowers data teams to leverage distributed compute infrastructure without managing backend complexity.

Coiled operates with a centralized control plane in our cloud account. All traffic to and from Coiled resources is encrypted, and authentication is enforced where appropriate.

Coiled avoids access to your data and your systems. Your compute and data access stay inside your AWS account. We give you a direct, secure connection and get out of the way.

Security of the Control Plane

- Coiled's control plane communicates with your AWS account via AWS API calls only.
- Coiled does not make any connections into your AWS account.
- More info: coiled.io/security

Data Handling & Privacy

- Coiled deploys resources in your VPCs using secure defaults, but with the option to configure VPC/subnet/security groups as needed for enhanced security or regulatory needs.
- Your data never leaves your environment. Coiled does not store or process customer data.
- Only lightweight telemetry (e.g., cluster runtime stats) is collected for observability, billing, and support.
- *Optional additional data (code and metrics) can be collected which enables us to provide enhanced support, this is not required and can be disabled.*

IAM Role & Access Justification

- Required permissions support provisioning and managing ephemeral compute resources.
- IAM permissions are minimally scoped and customizable per environment.
- All actions in your account are auditable via AWS CloudTrail.
- See https://docs.coiled.io/user_guide/setup/aws/reference#iam-policies for details.

Security Credentials

- SOC 2 Type II report is available under NDA.
- Coiled inherits compliance controls from AWS (SOC 2, ISO 27001).
- Proven history with regulated organizations: NASA, D.E. Shaw, Moderna, and more.