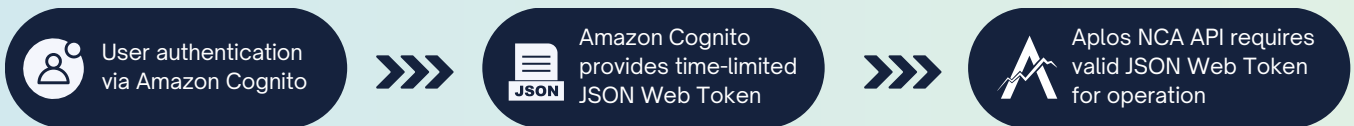# Security

Aplos NCA includes integrated security protocols and end to end encryption on all of your data and results. You can be confident that your data will be secure and access will be controlled by the best security protocols and procedures available.

Aplos NCA uses Amazon Cognito for user identity and access management

- Passwords are managed by Amazon Cognito. Aplos Analytics does not have access to passwords.
- Amazon Cognito processes more than 100 billion authentications per month
- Aplos can support Single Sign-on (SSO) with your company's federated authentication tool
- All Aplos NCA API commands are gated and require prior authentication

User authentication via Amazon Cognito ⟫⟫ Amazon Cognito provides time-limited JSON Web Token ⟫⟫ Aplos NCA API requires valid JSON Web Token for operation

Data encryption in transit, during analysis, and at rest

- All data transfers are encrypted using SSL/TLS protocols
- Analysis engine operates under encryption
- Input data and results are stored with KMS encryption using Amazon S3
- Team accounts include a separate AWS account with isolated S3 storage
- User data for individual accounts or users within a Team account is isolated using logical separation with S3 storage

Aplos Analytics, Inc. maintains policies and procedures to safeguard access to all systems and networks. Any access to customer systems to provide support requires prior authorization from the user and is recorded in access logs.