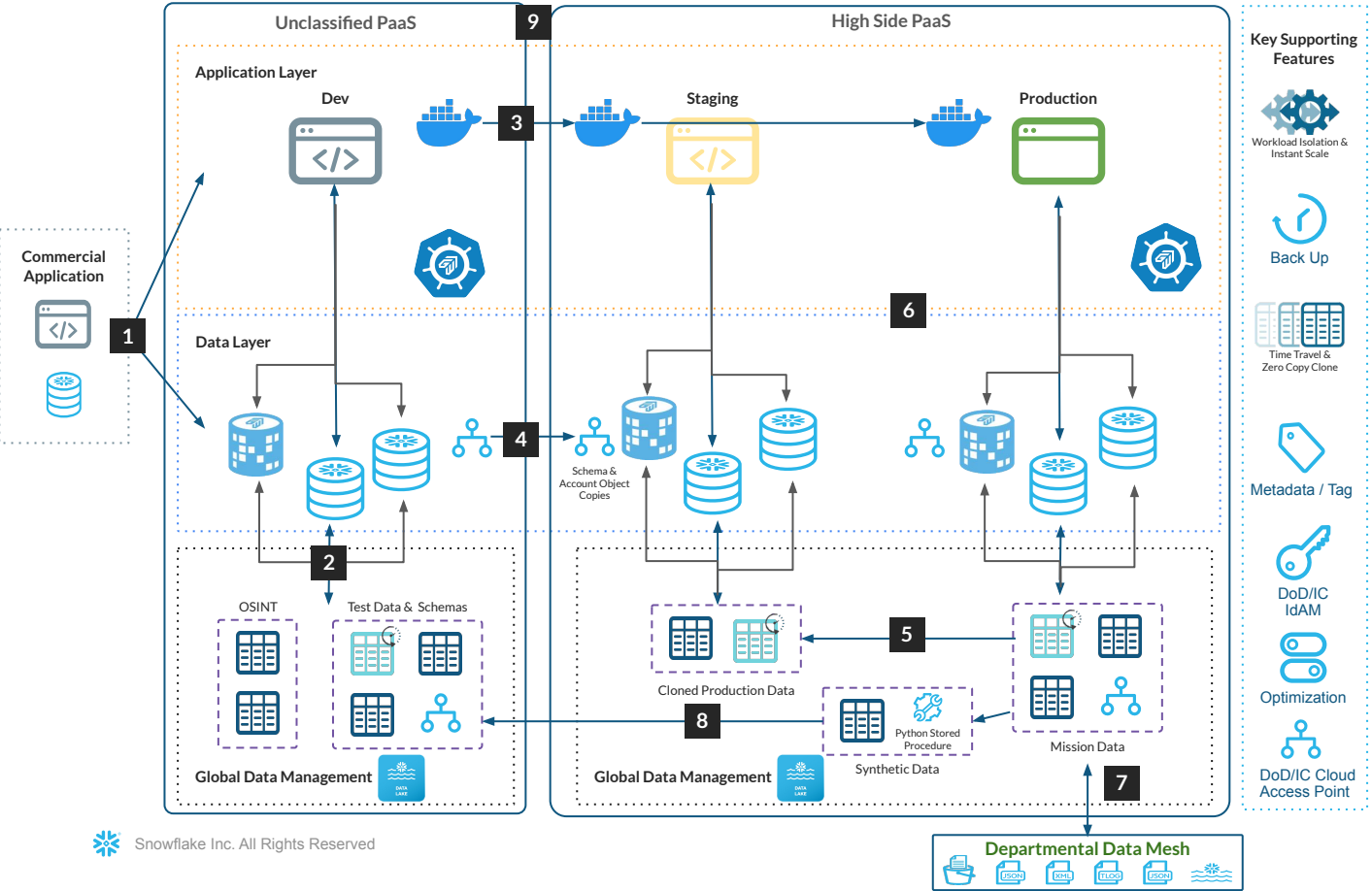
CONTINUOUS AUTHORIZATION TO OPERATE (cATO) REFERENCE ARCHITECTURE



Snowflake Inc. All Rights Reserved

OBJECTIVE

cATO through DevSecOps creates a process in which developers can iterate on software while maintaining government accreditation, without the long delays usually associated with the traditional accreditation processes. The benefit is rapid deployment and deployment of software critical to national security, and getting it into the hands of the users at the appropriate security level.

DESCRIPTION

1. Commercial Application Enters into Dev Environment for Refactoring and Reengineering
2. Tests on Low Side Data Transformed from Standardized Global Testing Data
3. Containers Moved into Staging
4. Data Schemas, Logic, and Account Objects Moved into Staging
5. High Side Staging Environment utilizes Cloned Production Tables for accurate near real-time mission data
6. Applications managed by Game Warden seamlessly connect to data managed by snowflake
7. Mission Data Connected into Data Mesh
8. Synthetic Data Generated for Replication into Low Side Testing
9. Application and Data layers operate within continuously monitored and accredited PaaS boundary

RELATED CONTENT

The reference architecture is based on the successful Game Warden DevSecOps platform developed by Snowflake partner Second Front, providing an innovative solution pipeline to DoD.