Command Cloud™ Data Segmentation

At Command Alkon, we ensure the highest levels of data security and privacy for Command Cloud through robust data segmentation and encryption practices.
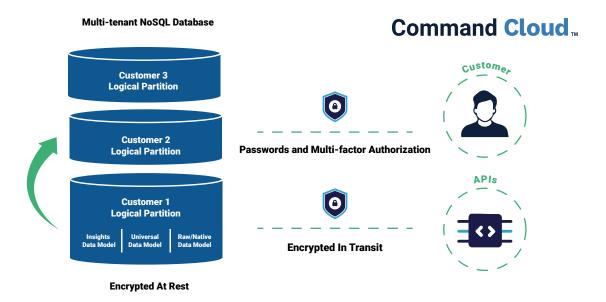
Data

All data is logically segmented using customer (tenant) mapping, ensuring that each customer's data is isolated and secure. Access to this data is strictly managed via role-based access controls, allowing only authorized personnel to access specific data based on their roles and responsibilities.

Security

We prioritize the security of data in transit by utilizing up-to-date TLS (Transport Layer Security) protocols, ensuring that all data exchanged between our APIs and our customers is encrypted and protected from interception. Additionally, all data stored in our systems is encrypted using FIPS (Federal Information Processing Standards) compliant encryption algorithms, meeting rigorous government standards for data security.

Hosting

Further enhancing our data security and segmentation measures, Command Alkon hosts Command Cloud in either the US or the EU, allowing customers to maintain data sovereignty requirements and ensuring compliance with regional data protection regulations.These comprehensive data segmentation and encryption practices demonstrate our commitment to safeguarding customer data and maintaining the highest standards of data security and privacy.

Multi-tenant NoSQL Database

Command Cloud™

Customer 3
Logical Partition

Customer 2
Logical Partition

Customer 1
Logical Partition

Insights Data Model | Universal Data Model | Raw/Native Data Model

Encrypted At Rest

Passwords and Multi-factor Authorization

Encrypted In Transit

Customer

APIs