Security Checklist

Access control	❏ Create unique user accounts for each individual and application that accesses the platform. ❏ Implement Role-Based Access Control and assign roles following a principle of least privilege ❏ Leverage strongest available authentication mechanisms ❏ Ensure secure storage and transfer of credentials or certificates ❏ Implement Multi-Factor Authentication for individual access
Secure network communication	❏ Replace self-signed certificates with external CA certificates ❏ Ensure all applications are using encrypted connections only and block insecure ports ❏ Enforce TLS with 'strict' encryption setting to encrypt all network traffic internally and externally. ❏ Only Enable IP Address Families as needed
Secure data storage	❏ Deploy encryption at rest ❏ Implement (FLE) Field-level Encryption ❏ Configure Secrets Management
Limit data exposure	❏ Remove unnecessary services and software ❏ Regularly scan for and protect sensitive data ❏ Control geographic distribution of data ❏ Leverage log redaction when collecting and transferring logs ❏ Deploy a comprehensive DR strategy utilizing offsite backups
Auditing	❏ Enable and configure auditing ❏ Review audit logs manually and programmatically for anomalies
Regular review	❏ Assess security from core to edge and perform regular security health checks ❏ Review enhancements provided with each new version of the Couchbase Data Platform ❏ Apply upgrades to the Couchbase Data Platform & SDK software, app frameworks, OS, networking infrastructure, etc.