cloudlocker

Security Overview

Cloudlocker is designed from the ground-up to be a secure storage platform for your legacy email and PST data. We leverage Microsoft Azure's services as the platform for CloudLocker. The Cloudlocker Service Management Center is located in Dallas, TX, and is secured with Biometric Two-Factor Authentication.

Data

- Data in Transit: All connections are forced to use TLS
- Data at Rest: All data is secured with AES 256-bit encryption, which is FIPS 140-2 certified
- Customer data is logically separated to ensure no access from one customer to another
- Data can be physically separated for additional costs
- Customer-managed keys can be supported in a physically separate environment (additional costs)
- Sessions automatically time out after 15 minutes of inactivity
- WORM can be enabled to ensure immutability during retention period

Personnel

- Extensive background checks are performed on all employees and regular security training is required.
- We implement a least-privilege policy to ensure access is granted only to the extent of each employee's responsibilities
- Roles within the application are managed by Azure Active Directory
- Only highly trained and credentialed individuals are able to manage the application and provide support
- Only US-based full-time employees provide support; We do not leverage contractors

Infrastructure

- Administrative functions are restricted by IP Address
- All actions are logged for auditing purposes
- Application usage is load balanced in Azure
- Administrative credentials are stored securely
- Multi-Factor Authentication is enabled for all administrative accounts
- Azure Active Directory is leveraged for authentication, including any logon restrictions, SSO, and multi-factor authentication
- Third-party penetration testing and code review
- ISO27001 certified

sales@cloudlocker.com | (845) 987-4645 | cloudlocker.com