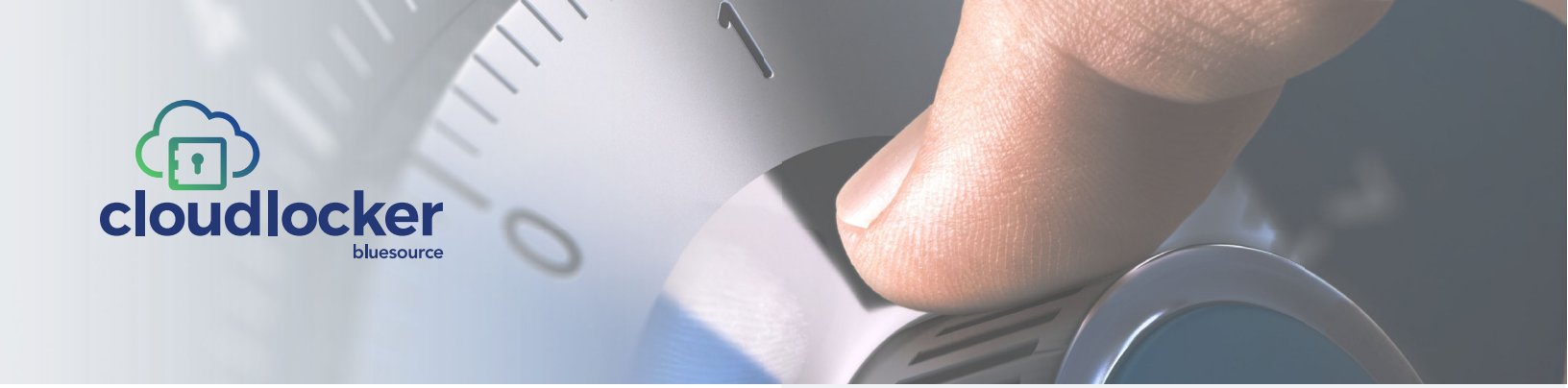

cloudlocker
bluesource

Security Details

Bluesource Cloud Locker 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 Bluesource CloudLocker. For information regarding the physical security of Microsoft Azure, please refer to azure.microsoft.com/en-us/overview/security/.

Our Service Management Center is located in Dallas, TX, and is secured with Biometric Two-Factor Authentication.

Infrastructure Security

- Inbound traffic is restricted to HTTPS over TCP443
- Administrative Functions are restricted by IP Address
- All requests to the system are secured with bearer tokens; no token, no response
- Application usage is load balanced in Azure
- Administrative credentials are stored securely via Azure KeyVault
- Multi-Factor Authentication is enabled for all administrative accounts
- Azure Active Directory is leveraged for Authentication

Data Security

- 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
- Keys are managed by Microsoft, and Bluesource employees have no access to keys
- Customer-managed keys can be supported for additional costs in a physically separate environment

Personnel Security

- Extensive background checks are performed on all employees
- Bluesource implements 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

bluesource

sales@bluesource.net
(845) 987-4645
bluesource.net