 **Environment Variables**: Store connection strings in environment variables to keep them outside the codebase and ensure they're only accessible to the environment where the application runs.

 **Configuration Files**: Store connection strings in configuration files (e.g., appsettings.json), and use encryption or secure access methods like Azure Key Vault or AWS Secrets Manager to protect them.

 **Secret Management Services**: Use secret management tools such as Azure Key Vault, AWS Secrets Manager, or HashiCorp Vault to securely store and retrieve connection strings, ensuring they are never hardcoded in the application.