Infrastructure Security

## User Authentication/Authorization

All user access to infrastructure is managed through AzureAD SAML and Azure AD Domain Services SAS solutions.

AzureAD will grant access to Roles within the AWS CDAP Infrastructure.

Admin User access to any secure CDAP networks will be by connection to AWS Client VPN service using AzureAD SAML authentication with MFA verification.

All User Infrastructure Access will require use of an MFA token.

No AWS IAM user accounts will be used for CDAP Infrastucture access.

Temporary AWS IAM credentials will be generated using AzureAD SAML authentication for any AWS CLI admin tasks.

## Application Deployment

All application deployment into the AWS CDAP environment will be completed using AWS CodePipleines, managing required IAM role access for each of the Dev/Test/Prod Application Deployment Accounts.

## Security Logging

All AWS accounts in the CDAP platform will forward AWS CoudTrail Audit Logs to the CDAP AWS Audit Account, where Admins will have read-only access for review purposes only.

AWS Guard Duty service will provide security anomaly detection, reporting any alerts to the Operations team Alerts notification channel.

Azure AD Audit Trail to be saved to a Secure Azure Storage Space with Read-Only user access.

Azure AD provides advanced identity protection providing anomalous activity reporting.