IDVerifact Application Security Overview

IDVerifact has the following application security measures for the design platform

- Access is available via user credentials which can be their specified username and password of leverage Auth0 with providers like Google, Microsoft etc.
- The Composition workflow is based on the entitlements assigned to the tenant users which are classified in four groups
    - Business Analyst: User who can create and edit a composite API
    - Finance Approver: User who can view a composite API and provide approval for finance review.
    - Technical Resource: User who can view the composite API, generate test API key for the composite API, and provide technical parameters for testing. Additionally, they can also add test results on the IDVerifact platform
    - Deployer: User who can view the composite API and generate production API key for the composite API, provide technical parameters for production instance and deploy and composite API.
- The about groups are associated with a set of permission, however a user can also be provided discrete set of permission for e.g., a user who can only view a composite API and add test results etc.
- A user from a particular tenant cannot view the composite APIs of another tenant.

IDVerifact Composite Identity API security measures are as follows:

- The Composite Identity API requires a unique API key for test and production for the tenant to call the composite API.
- Additionally, the tenants can also provider domain / IP address that will be recorded as whitelisted domains/IP address so Composite API call will only get executed if the API header has the correct API key and is triggered from a domain / IP Address which is whitelisted on the IDVerifact platform

IDVerifact Platform technical security implementation:

- IDVerifact platform is deployed on Google Cloud Platform and appropriate entitlement are assigned to the dev-ops team members to perform their designated tasks.
- IDVerifact platform encrypts all the data at rest via standard database and disk encryption and all data in flight via HTTP(S) with TLS 1.1
- IDVerifact platform database encryption key is recycled every 90 days for additional security to ensure that it meets the InfoSEC standards for ISO 27001