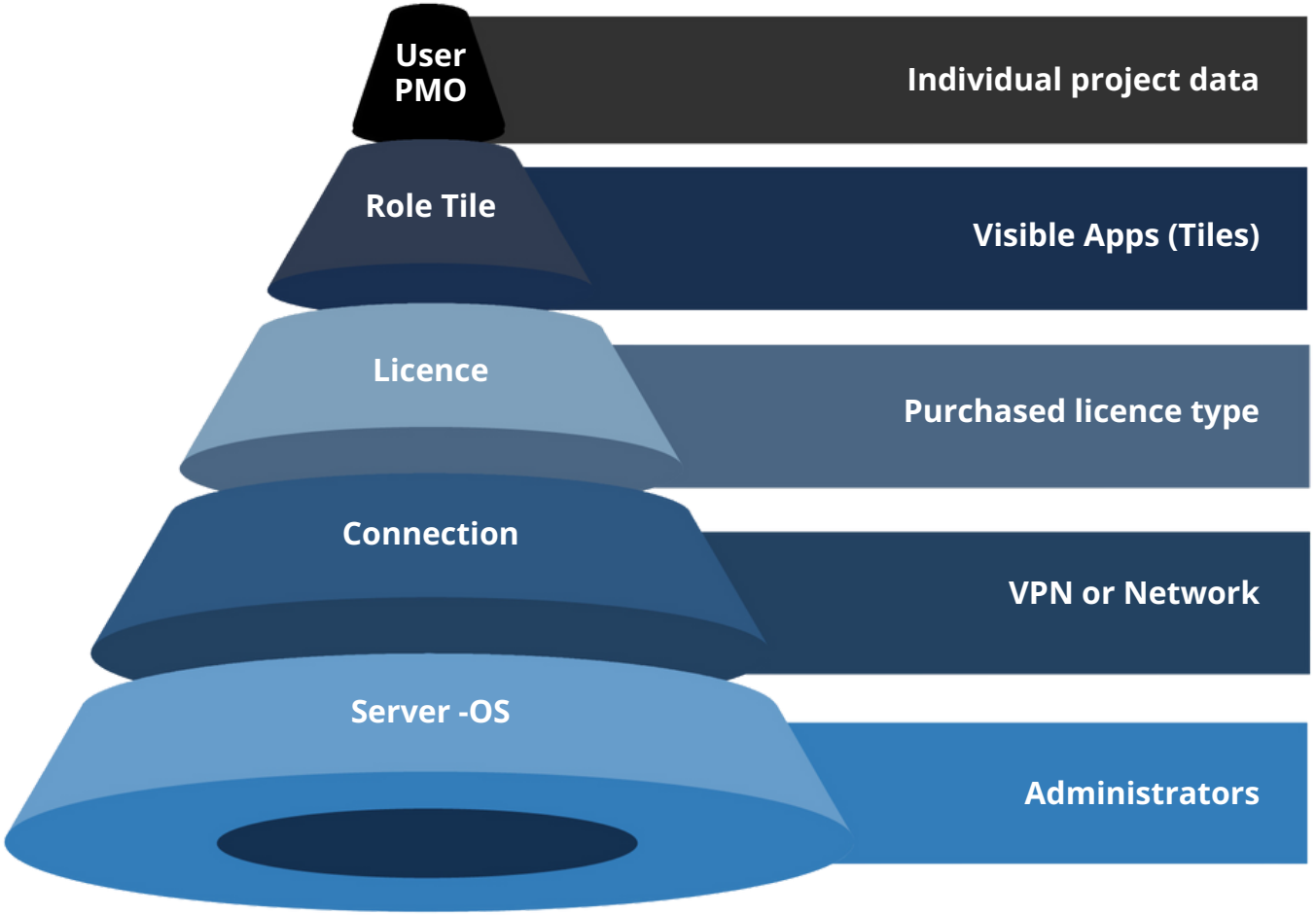
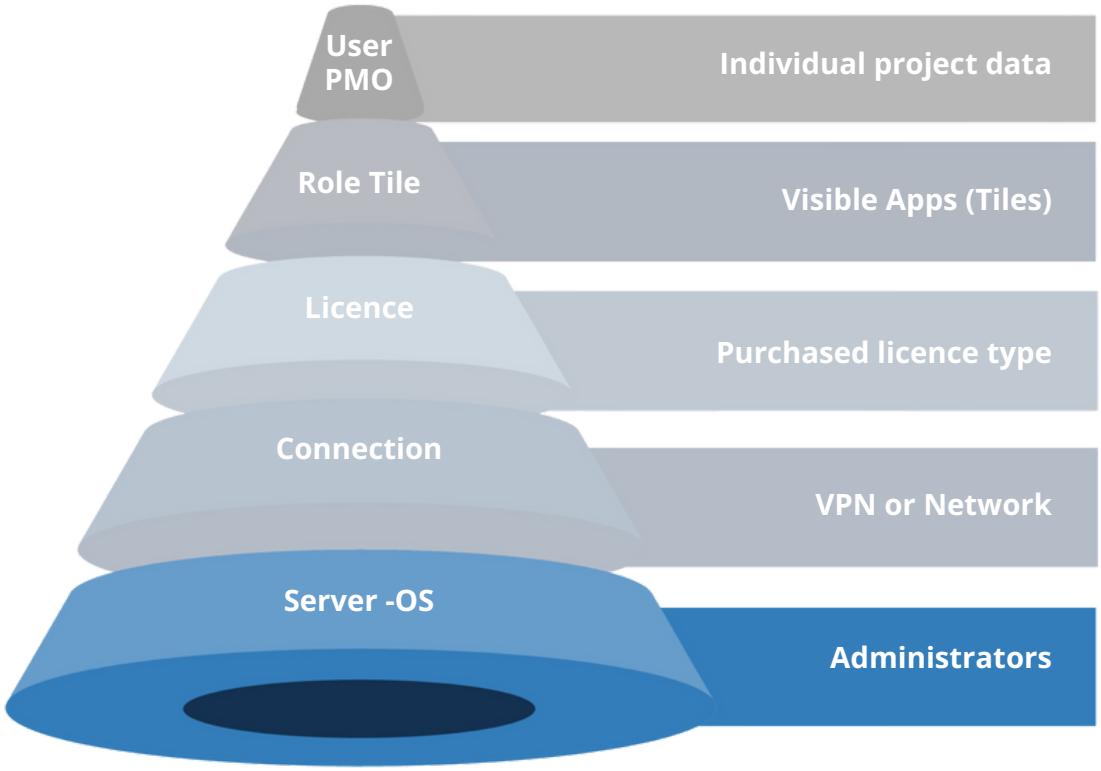
THE CAN DO AUTHORISATION CONCEPT



THE CAN DO AUTHORISATION CONCEPT



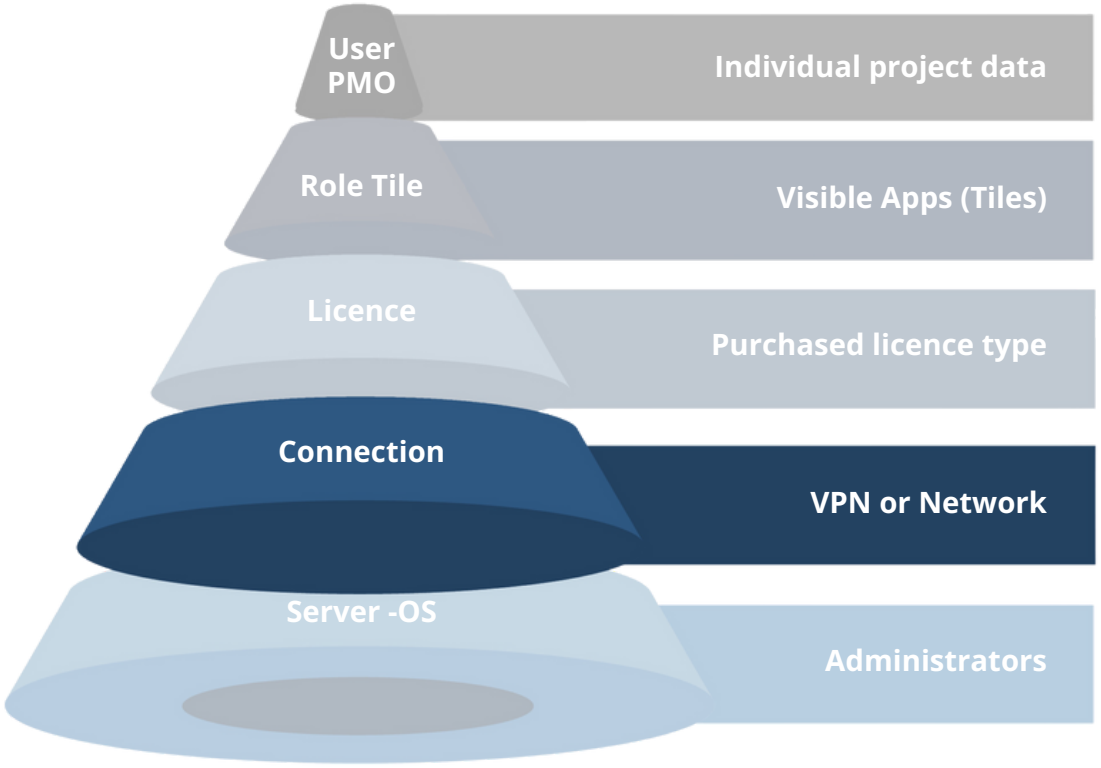
On premise operation in the data centre or private cloud of the customer

- Access only for internal administrators of the customer
- Security is ensured by client staff
- All servers included, also data base servers

SaaS Cloud Operation AWS

- Access only for authorised Can Do administrators
- No access to data base contents

THE CAN DO AUTHORISATION CONCEPT



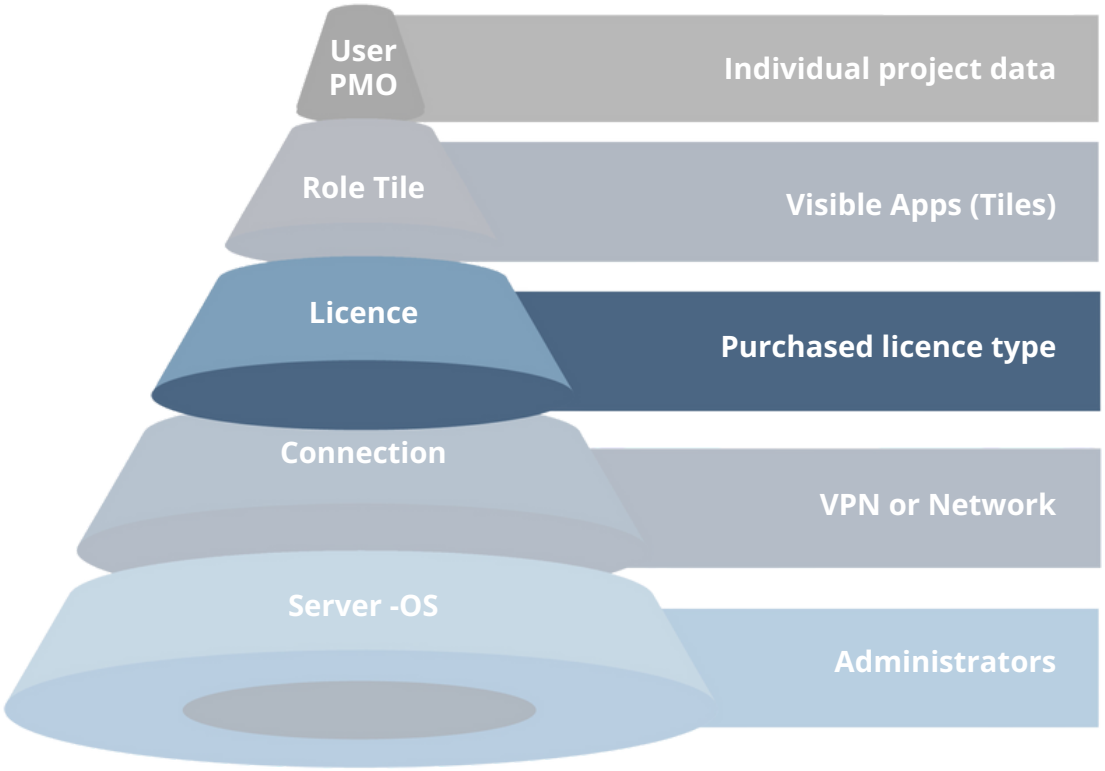
On premise operation in the data centre or private cloud of the customer

- Protection HTTPS protocol
- Additional VPN connection

SaaS Cloud Operation AWS

- Protection HTTPS protocol
- Additional VPN connection (optional)
- Additionally only authorised IP addresses (optional)

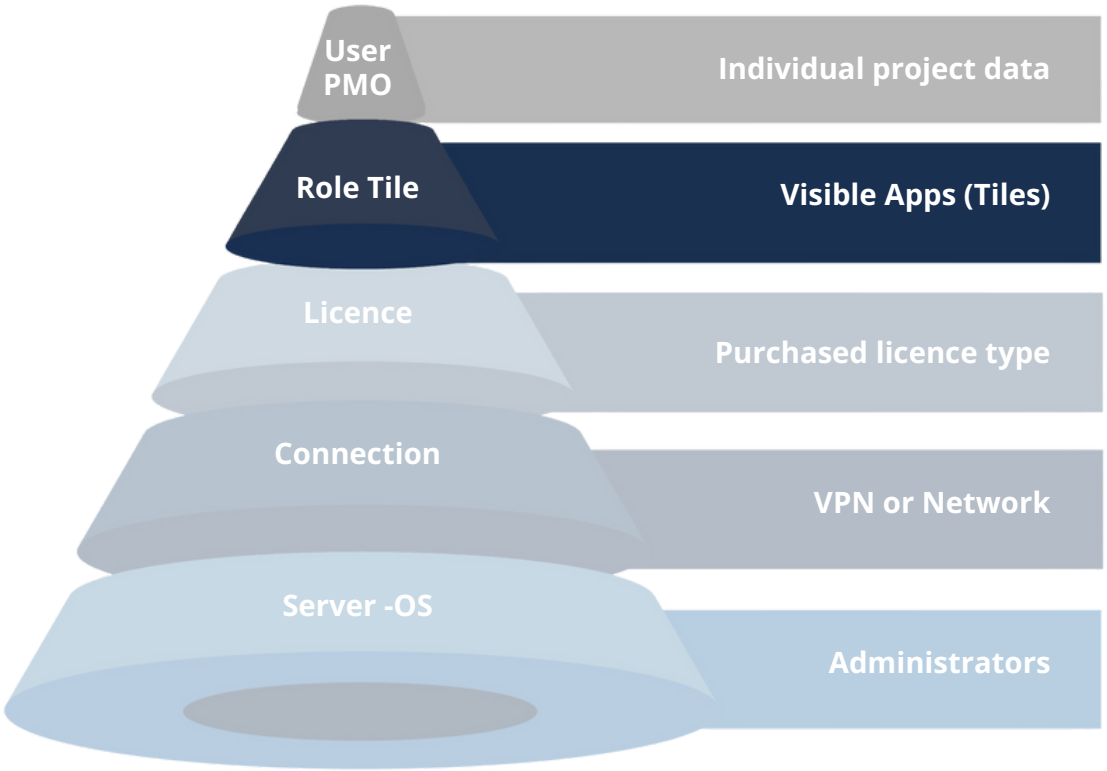
THE CAN DO AUTHORISATION CONCEPT



Purchase or Lease

- User must have a valid licence
- Licence check via encrypted licence key on the server
- Licence key can only be created by Can Do
- Users are created within the scope of the licence by the customer itself
- No access to user data by Can Do (in all operating modes)

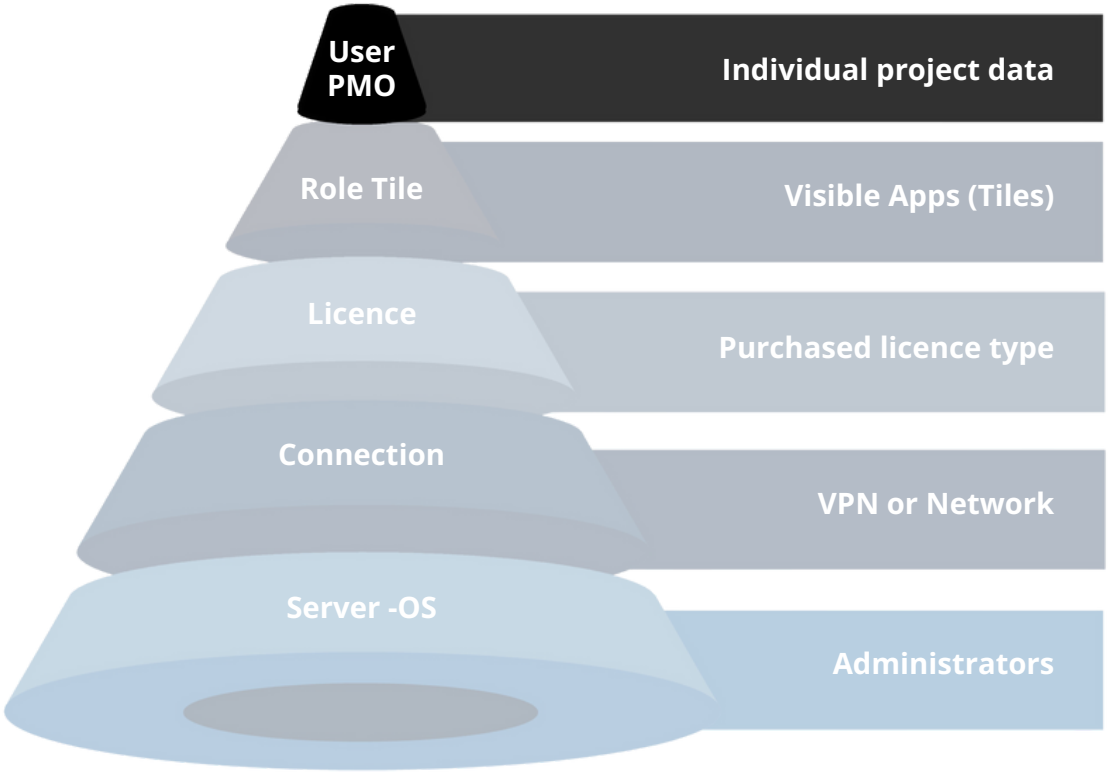
THE CAN DO AUTHORISATION CONCEPT



Role Model

- The role model describes which tiles the user has access to.
- Approx. 50 role models available by default
- Role models can be adapted by the customer / Can Do
- Assignment of the user to the corresponding role by the customer

THE CAN DO AUTHORISATION CONCEPT



Permissions

- Model of access to special object data is available (default)
- Access models can be adapted (by clients/Can Do)
- Models regulate each field and action per object
- Accesses (privileges) are: Read, Write, Change, Delete
- User/privileges can be assigned for all objects/users
- User/privileges can be grouped together:
  - Example 1: Project managers cannot change portfolios.
  - Example 2: Department managers cannot change defined projects.
  - Example 3: Employees cannot see resource utilisation of other employees