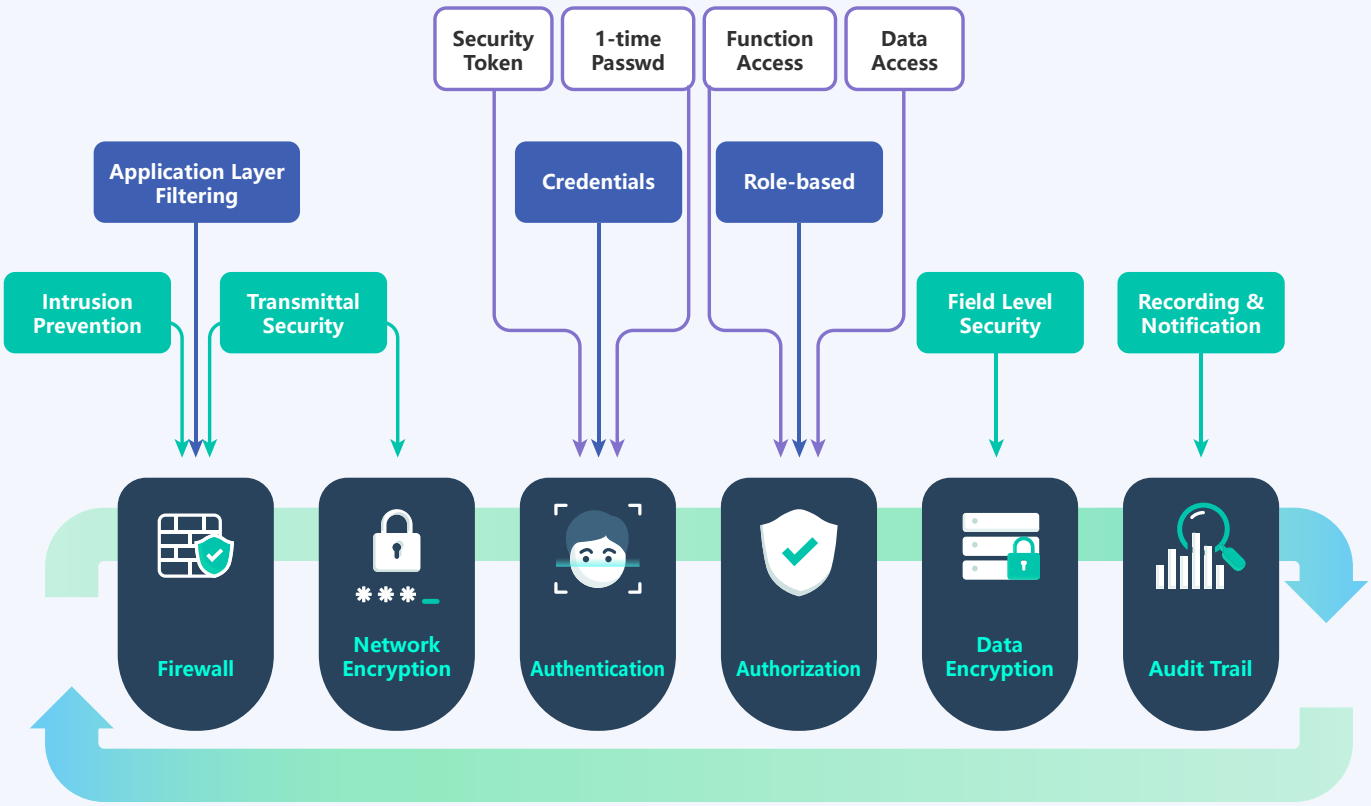
Security

Lower cost
and higher efficiency

Wisage Technology Limited（Hong Kong）
2702-6 Lucky Commercial Center 103-9 Des Voeux Road West
+852-6919-6665

Security



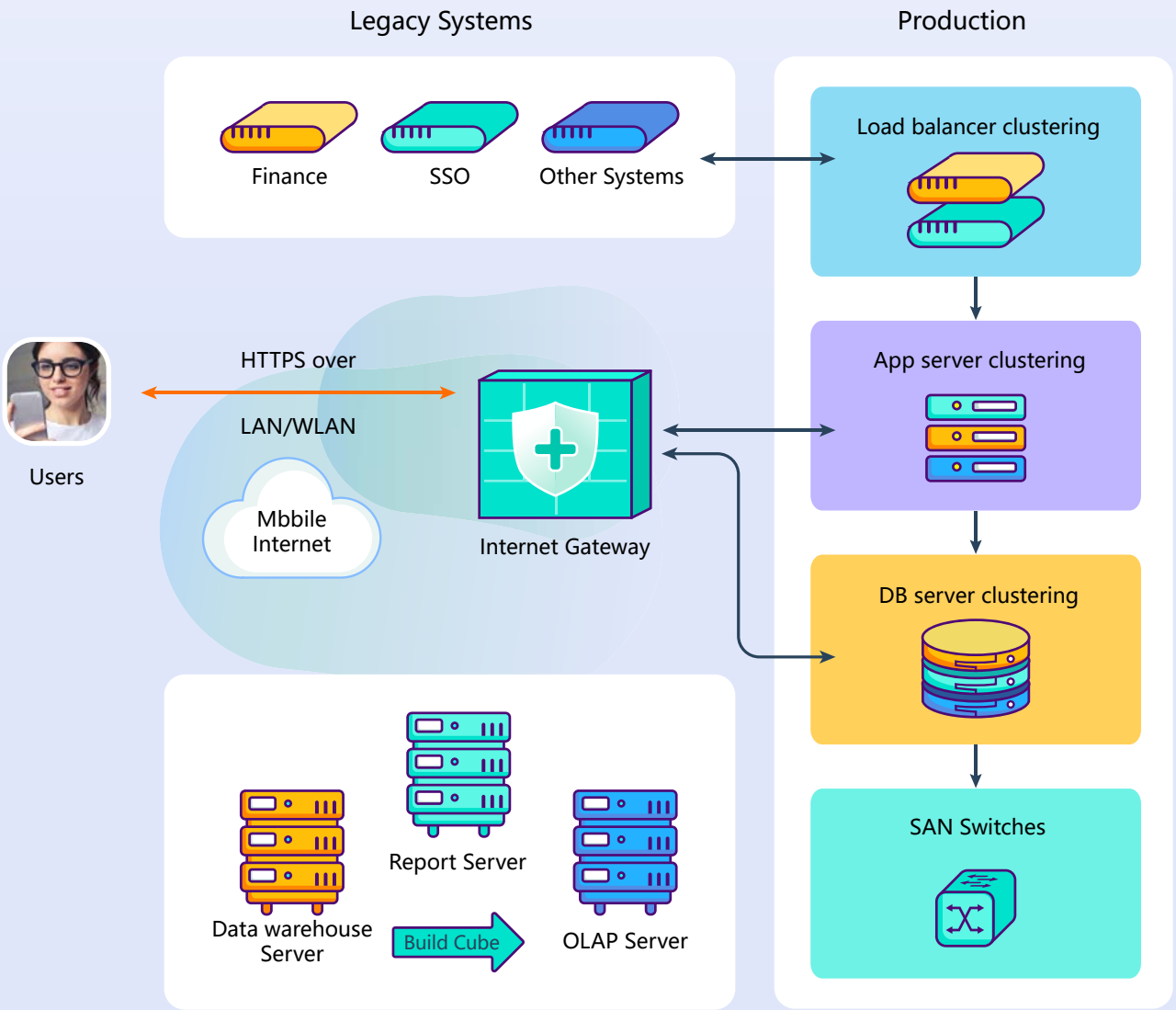
supports N-tier architecture which allows firewalls to be set up for packet inspection and application filtering to protect the servers in each layer against malware and intrusions.

uses HTTPS for transmittal security and supports Multi-factor Authentication (MFA), separate role-based authorization for function and data, different methods for data encryption and provides the audit trail mechanism to log actions, detect unwanted behaviors and send out alerts.

Network Security

Transmittal Encryption:

uses HTTPS for secure communication over computer networks. HTTPS is a mature technology that is widely used on Mobile Internet. In HTTPS, the communication protocol is encrypted by Transport Layer Security (TLS), or formerly, its predecessor, Secure Sockets Layer (SSL).

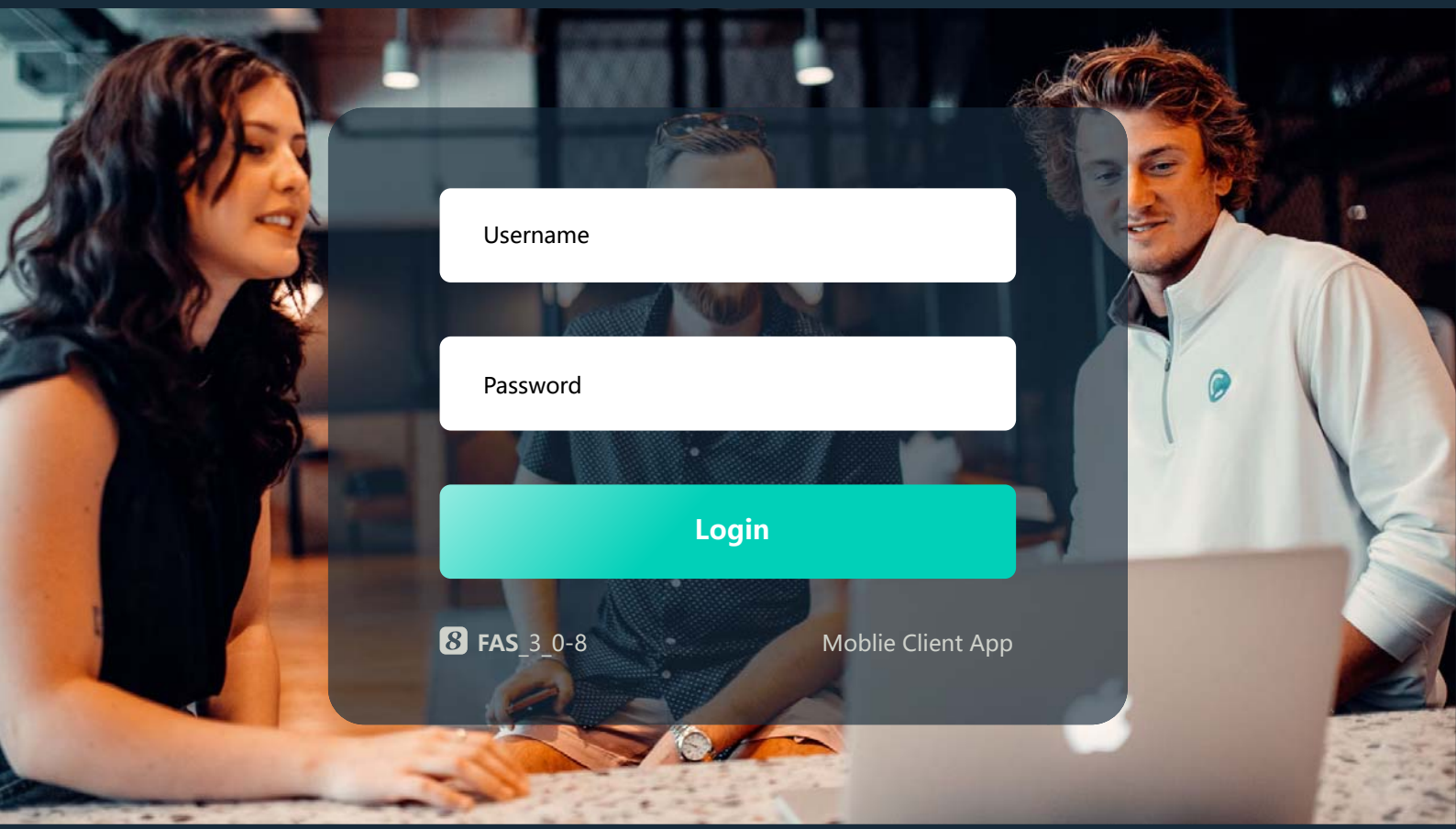


Device Address Access Control:

This is for the organizations who want to control who can access to the system by IP address, Network Segment or device access controlled by firewall.

Multi-factor Authentication (MFA)

supports different authenticator apps (e.g., Google Authenticator, Microsoft Authenticator) and different types of security tokens for MFA to provide an additional layer of security and makes it harder for attackers to gain access to a person's devices and online accounts, because knowing the victim's password alone is not enough to pass the authentication check. MFA has long been used to control access to sensitive systems and data, and online services are increasingly introducing MFA to prevent their users' data from being accessed by hackers who have stolen a password database or used phishing campaigns to obtain users' passwords.



Single Sign On (SSO) Integration:

supports the integration with SSO such as Windows Active Domain, LDAP, CAS, Open AM and Oracle OAM.

Third-party Authentication Integration:

has the pre-built integration with i-Sprint Authentication Service.

Password Security Management

Password Strength & Protection Policies:

allows the security officer to determine and set the following password strength and protection policies:

- Mandatory password change for initial user login
- Mandatory periodical user password change policy
- Password minimum length enforcement
- Password minimum number of alphabets enforcement
- Password minimum number of digits enforcement
- Password minimum number of special characters enforcement
- Word disallowed in password
- Number of repetitions of the password
- Login time control by roles/users
- Suspend inactive users
- Password age constraint

Data Encryption

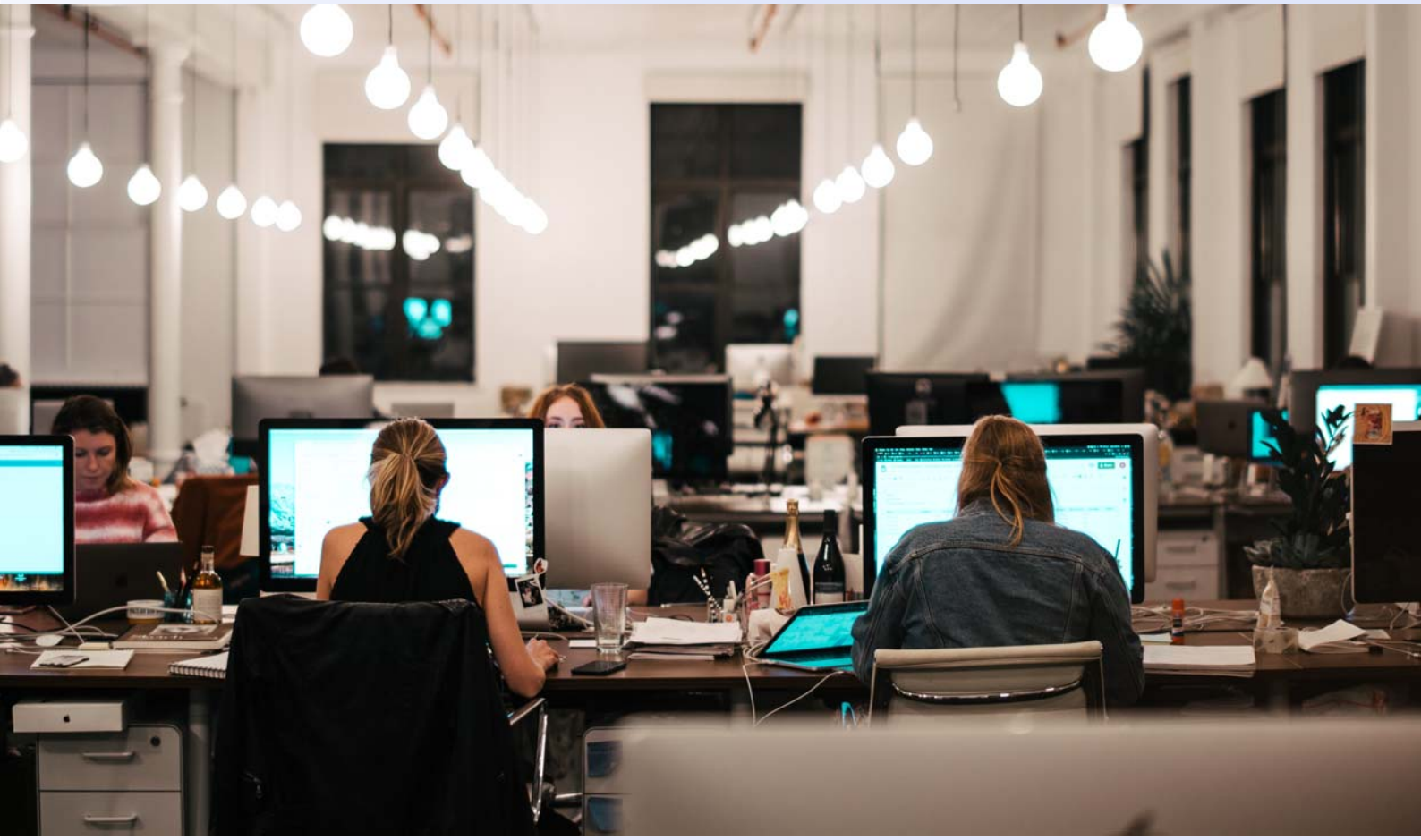
supports the following for data encryptions:

- Advanced Encryption Standard (AES) 256 for file and database encryptions
- Secure Hash Algorithm (SHA) 256 is used for password hashing
- Pretty Good Privacy (PGP) 4096 is used for license file encryptions

Role Based Access Control

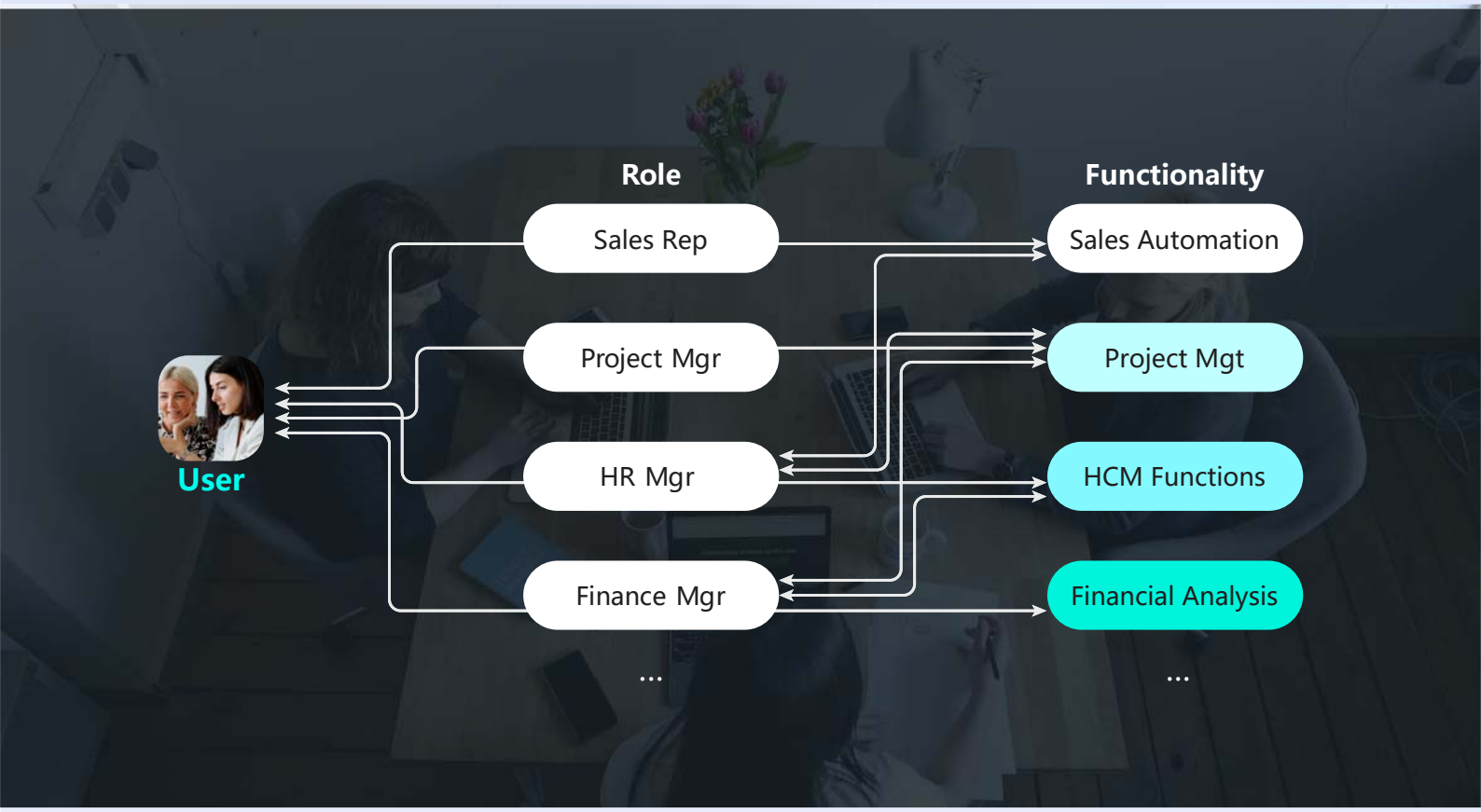
One of the key concepts in placing controls over functions and data of systems is segregation of duties. Segregation of duties serves the following 2 key purposes:

- Ensuring that there is oversight and review to catch errors
- Helping to prevent fraud or theft because it requires two people to collude in order to hide a transaction



supports segregation of duties and provides Role Based Access Control (RBAC) to control accesses by entitlement and/or authorization. In , when the user is being assigned to or unassigned from a role, she will be automatically entitled to or debar from the access rights associated with that role. The user can also gain or lose additional access rights that are authorized to or removed from her by higher authority.

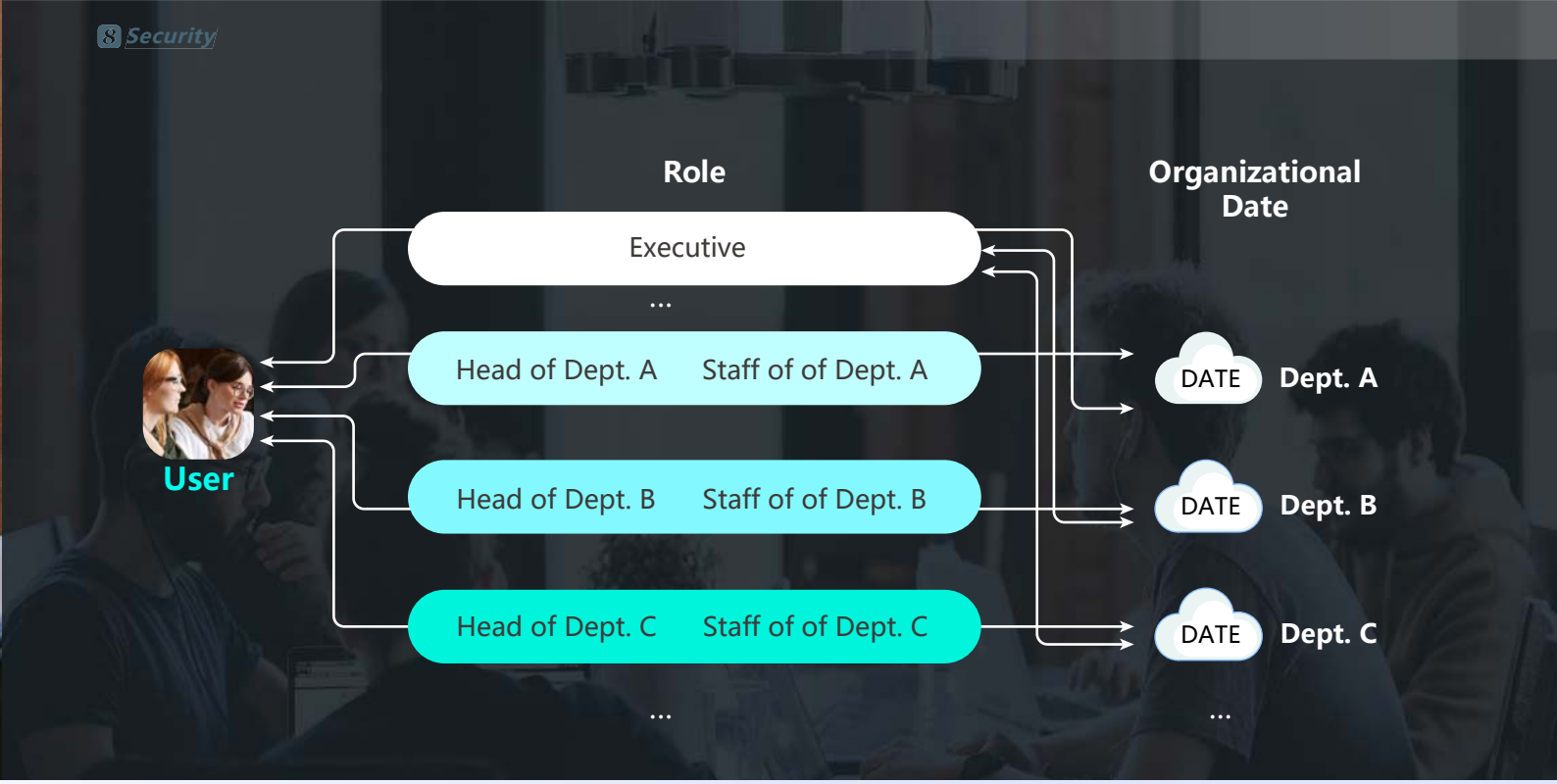
Due to the fact two managers of two different departments might need to have the same access rights to system functionality but different access rights to data (e.g., Manager A of department A needs to access department A's data and manager B of department B needs to access department B's data), supports separation of access rights to system functionality and data (e.g., Manager A and manager B have the same rights to functionality but different data access rights to data).



RBAC: Functional Access Entitlement

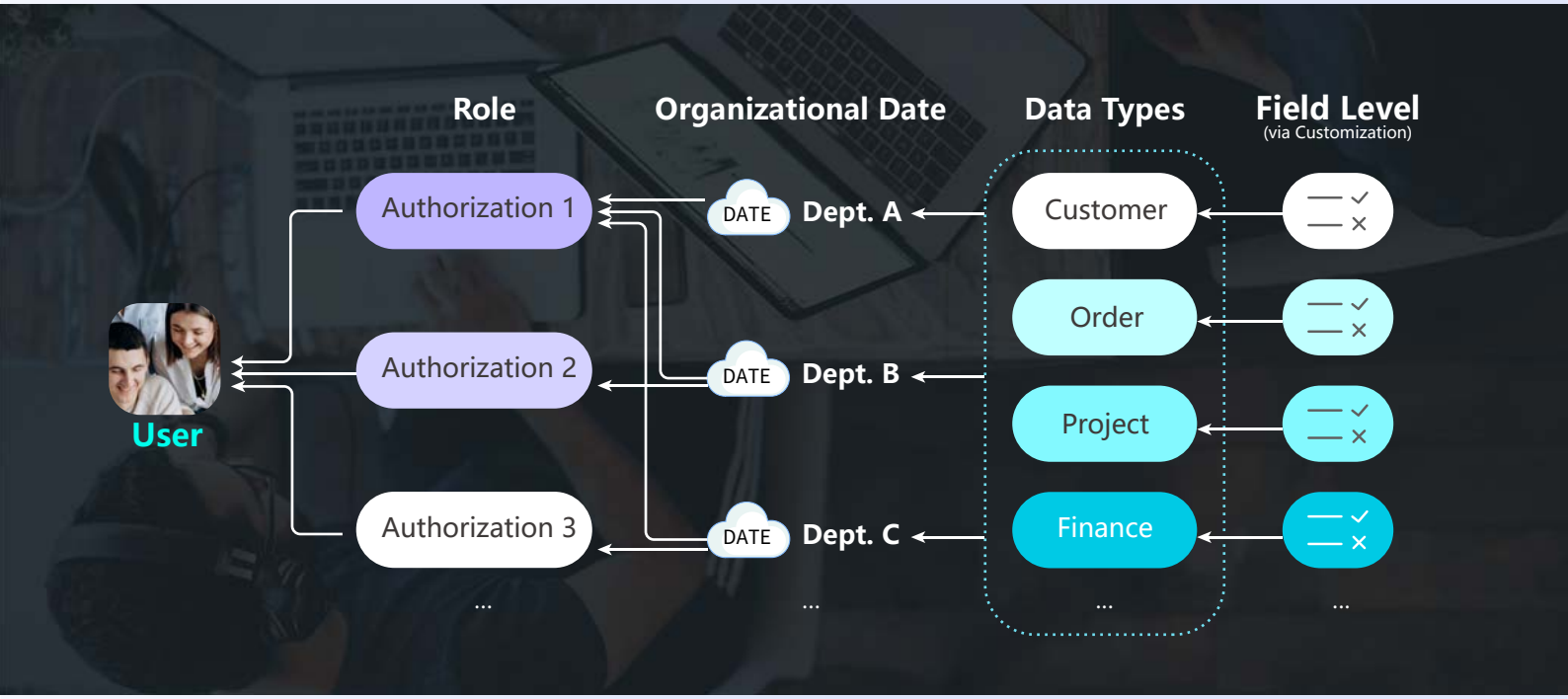
allows different roles (e.g., Sales Rep, Project Mgr., HR Mgr. and Financial Controller) to be defined and each user is assigned to one or multiple roles.

The user's functional access rights are determined by the roles assigned to her.



RBAC: Data Access Entitlement

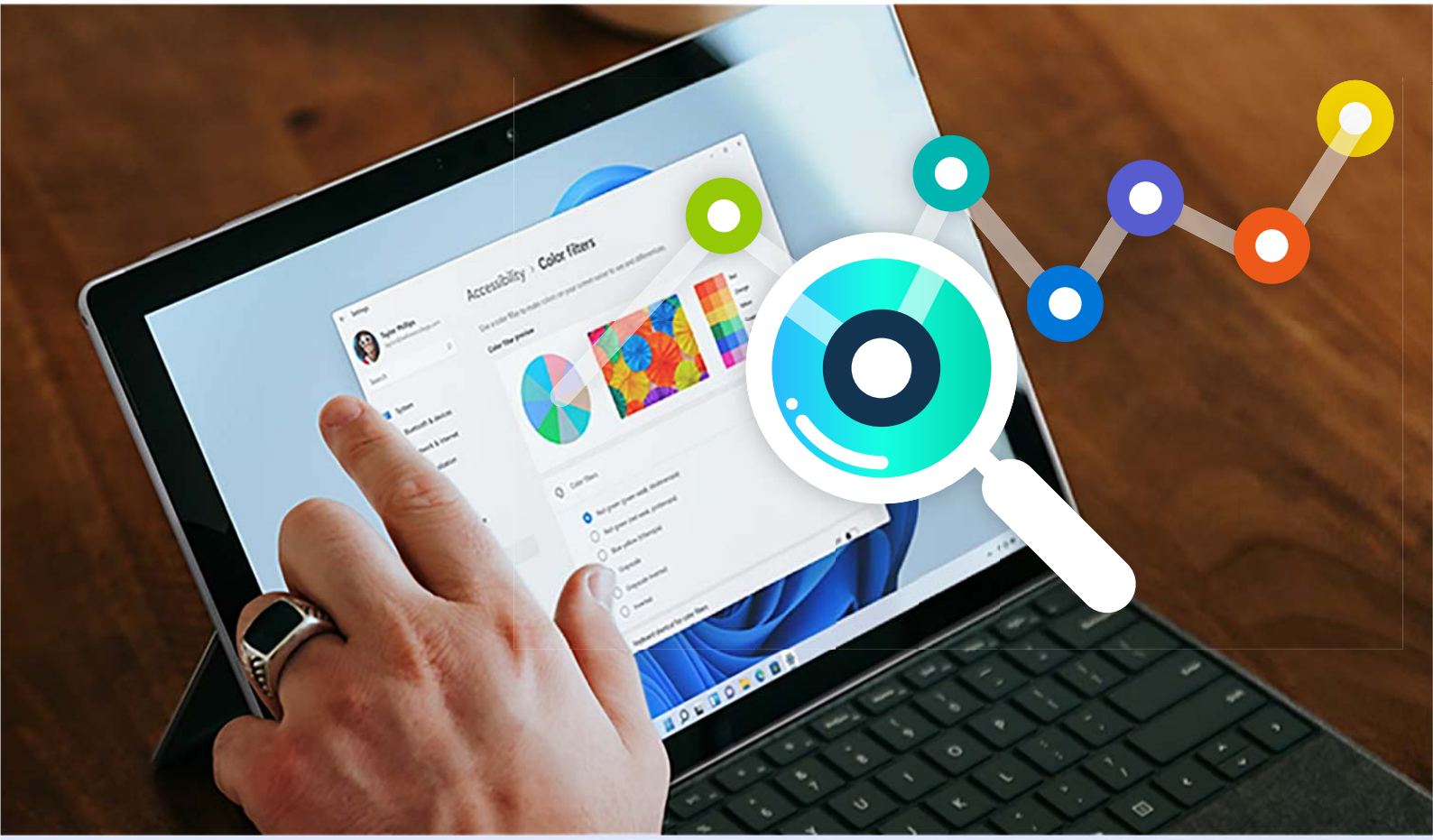
Security allows different roles (e.g., Executive, Division Manager, Department Manager) to be defined and each user is usually assigned to one role. The user's data access rights are determined by the roles assigned to her.



RBAC: Data Access Authorization

Security supports authorizing users extra data access rights by the users (e.g., administrator) who have the authorization authority. The authorization can be done in the organization data level, data type level and field level.

Audit Trail



provides unalterable and undeletable audit logs which contains the chronological records of all changes made to each business object including:

- Who makes the change
- Time of the change
- Data difference before and after the operation

The log history of user actions, interactions and transactions also includes the network address (IP) of each user.

8 can provide best combination of standard products & redevelopment services for enterprise management and over 500 corporations in Asia are using our following modules on-premises or SaaS:

- **SRM** : Supplier Management, e-Procurement and e-Tender
- **PPM** : Project and Portfolio Management
- **CRM** : Corporate Client CRM and Consumer CRM
- **Timesheet** : Resource Time and Cost Management
- **New Way** : Visual Agile and Lean
- **Service** : Service Management
- **EDMS** : Electronic Document Management System
- **OA** : Office Automation
- **HCM** : Human Capital Management
- **All-in-one** : Enterprise Full Automation

Wisage Technology Ltd.

8Manage.com

info@wisagetech.com

+852-6919-6665