Access Controls

Max McCarty

@maxRmccarty https://lockmedown.com

Overview

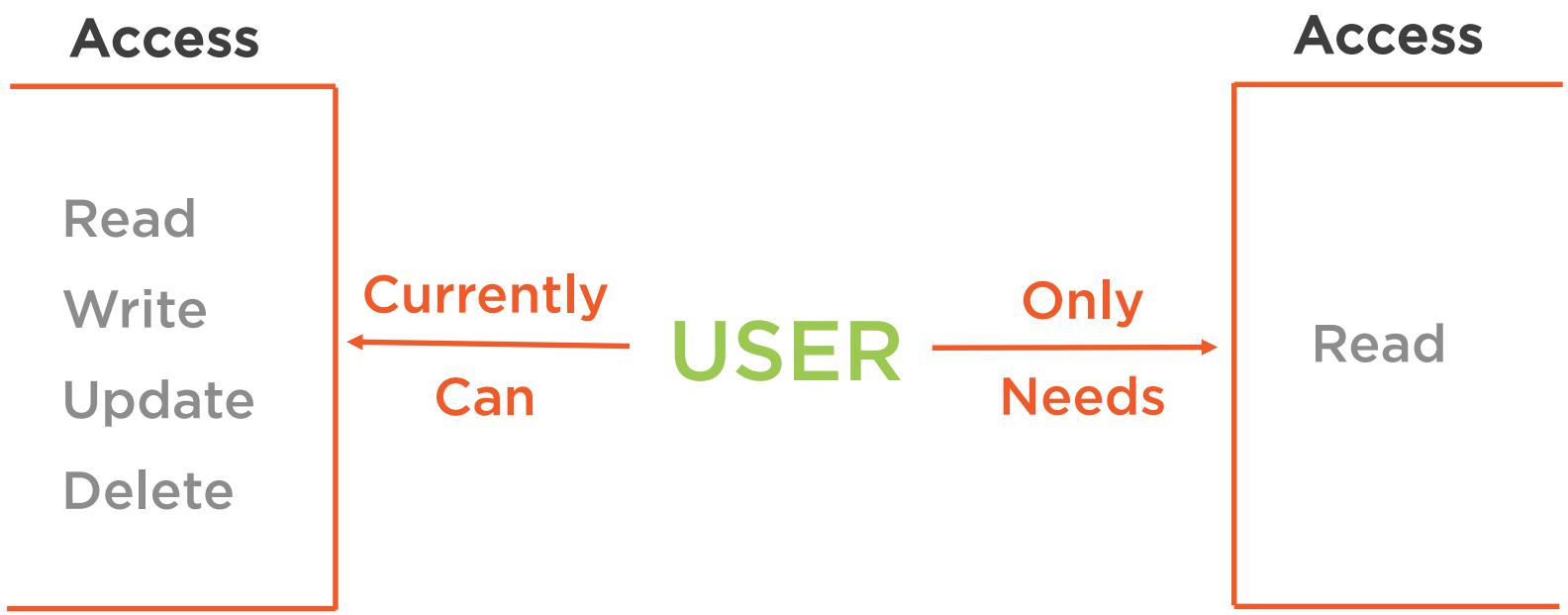
- Principle of Least Privilege
- The Problem with Database Access
- Restricting Application Database Access
- Role Based Access Control
- Function Level Controls (with RBAC)
- Server-side Function Level Control Failure
- Access Control Misconfiguration

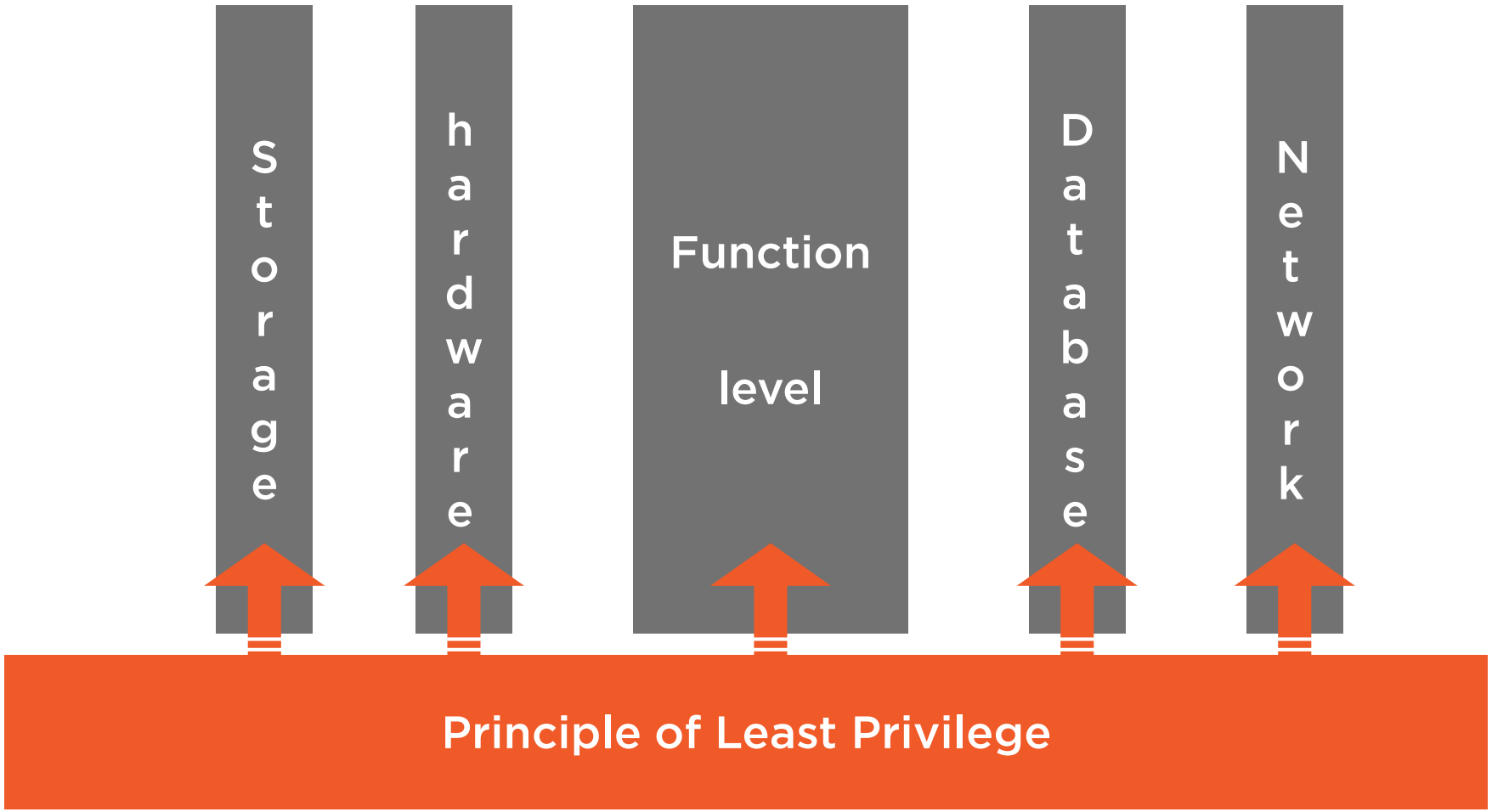
Principle of Least Privilege

Principle of Least Privilege

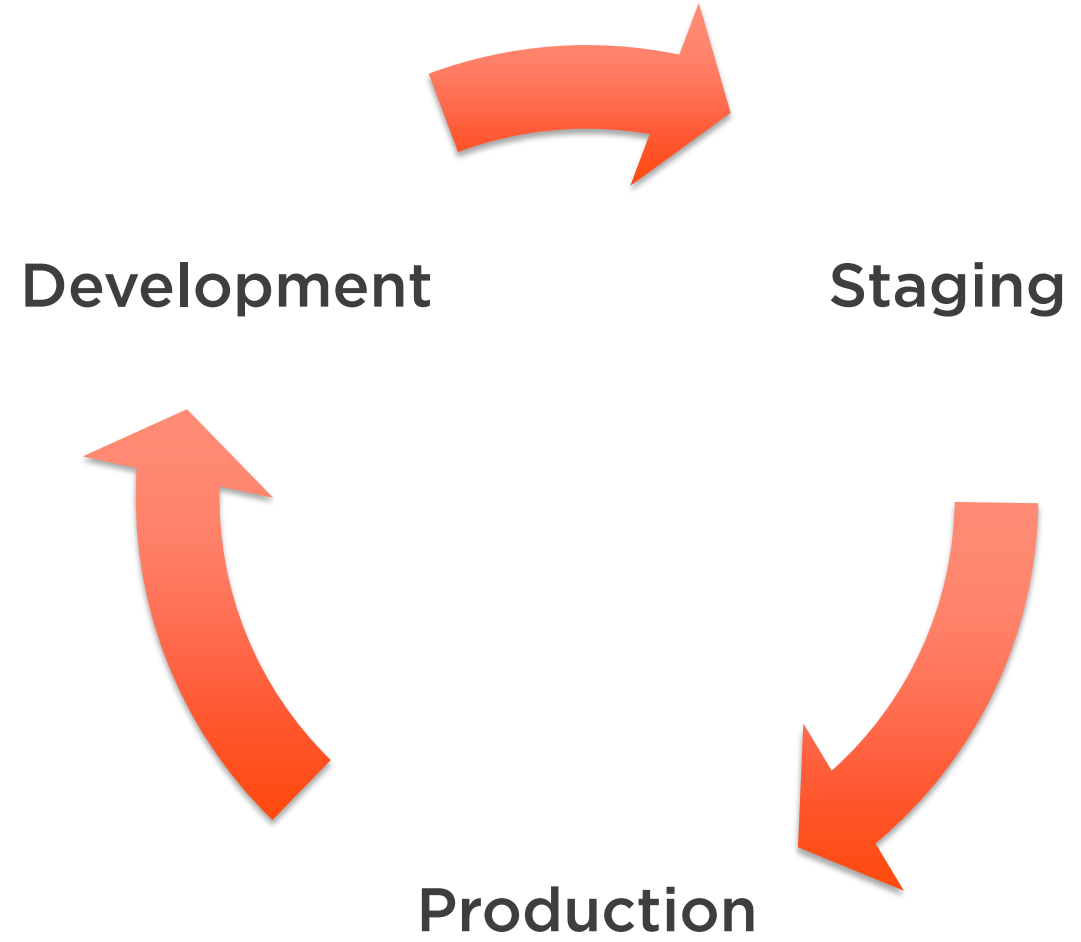
Every program and every privileged user of the system should operate using the least amount of privilege necessary to complete the job.

—Jerome Saltzer, Communications of the ACM

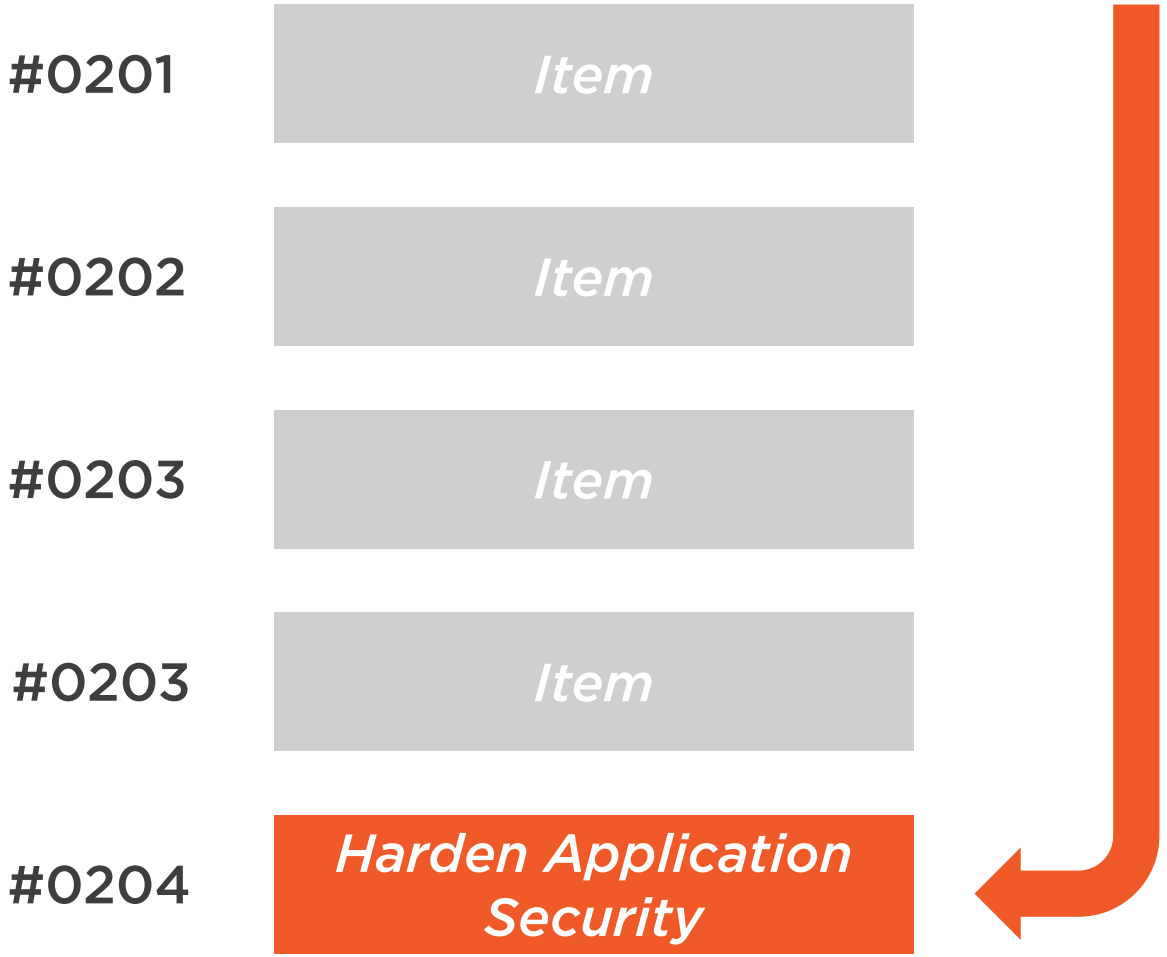

Access
Read
Write
Update
Delete
Currently
Can
USER
Only
Needs
Access
Read


Storage
hardware
Function level
Database
Network
Principle of Least Privilege

Application Development Life Cycles



Product Backlog



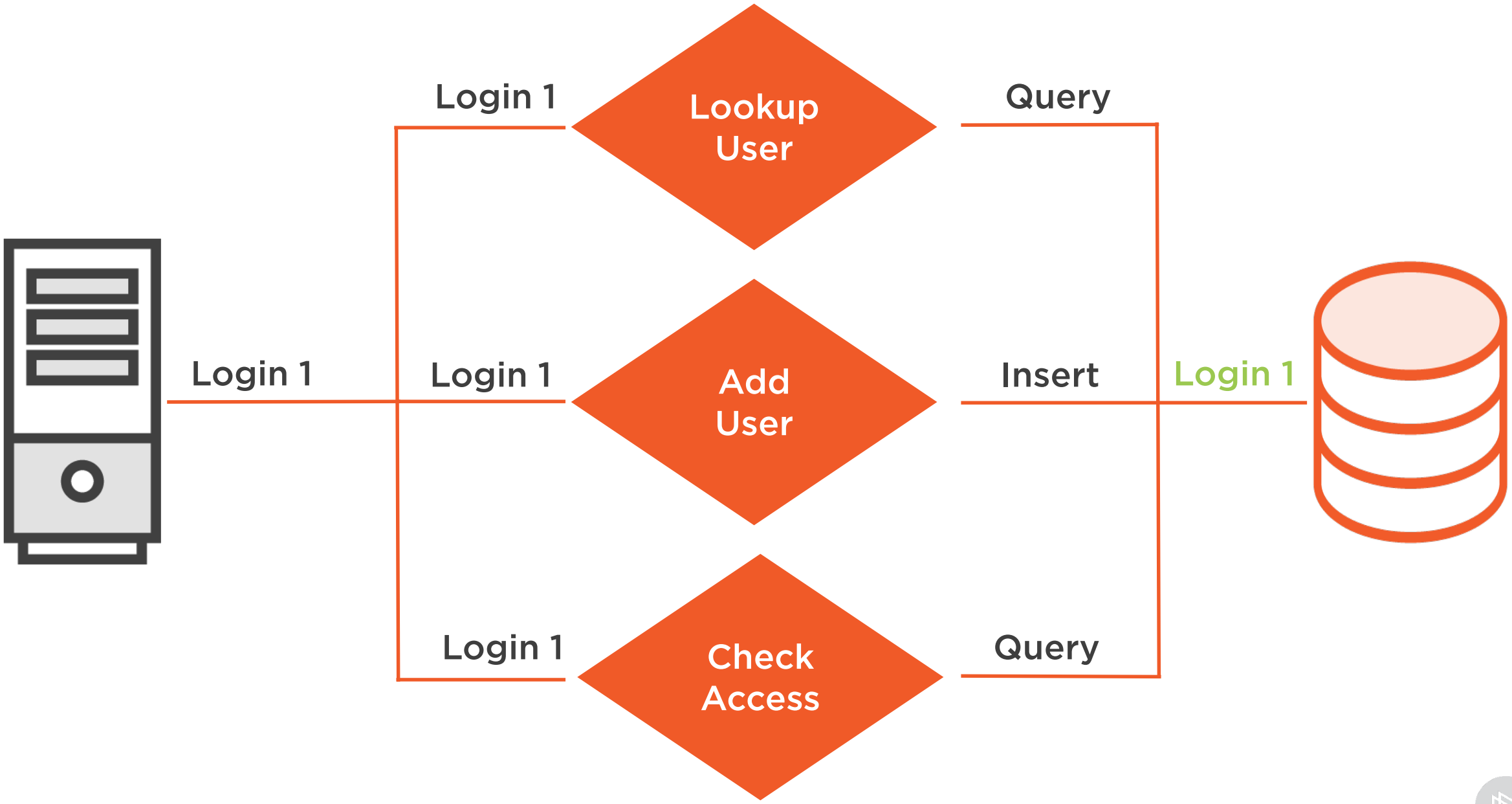
Developers

Architects

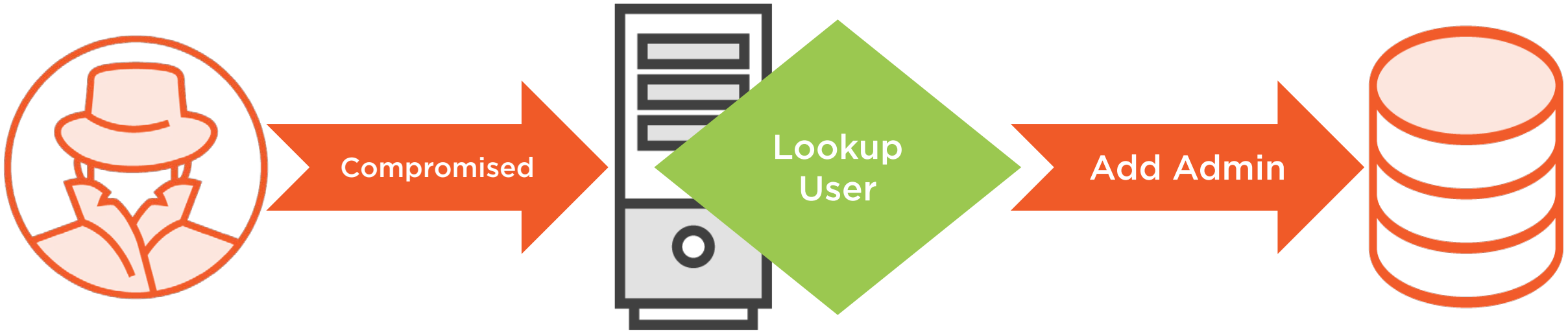
Testers

Beta Testers

The Problem with Database Access


Login 1
Lookup User
Query
Login 1
Login 1
Add User
Insert
Login 1
Login 1
Check Access
Query

Compromised System with Elevated Access



Role Based Access Control

Access Control Methods

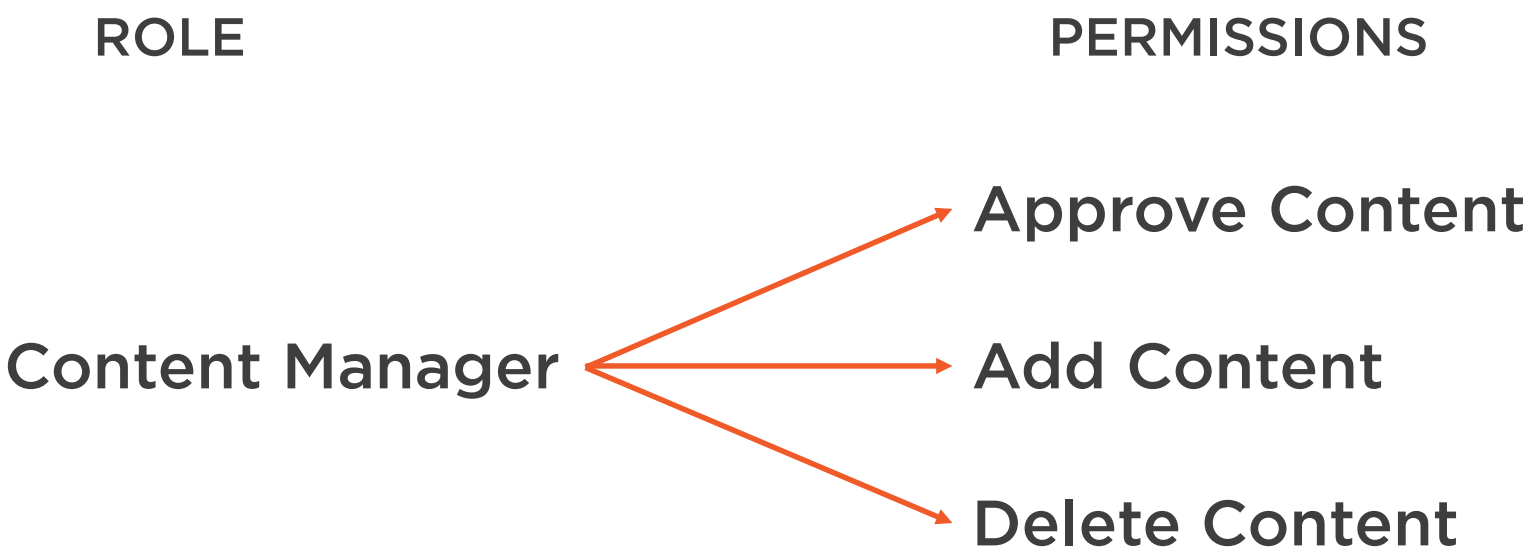
Mandatory /
Discretionary
Object Based

Identity Based

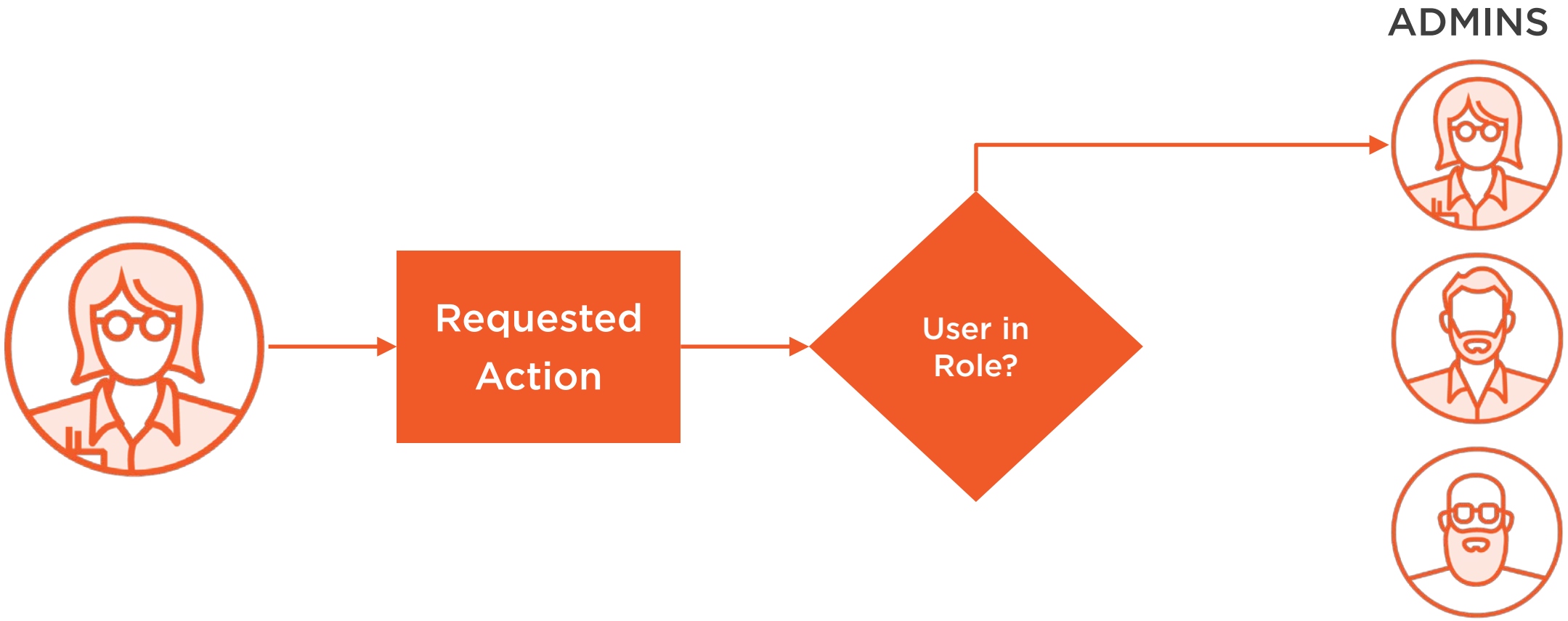
Role Based

Role Based Access Control (RBAC)

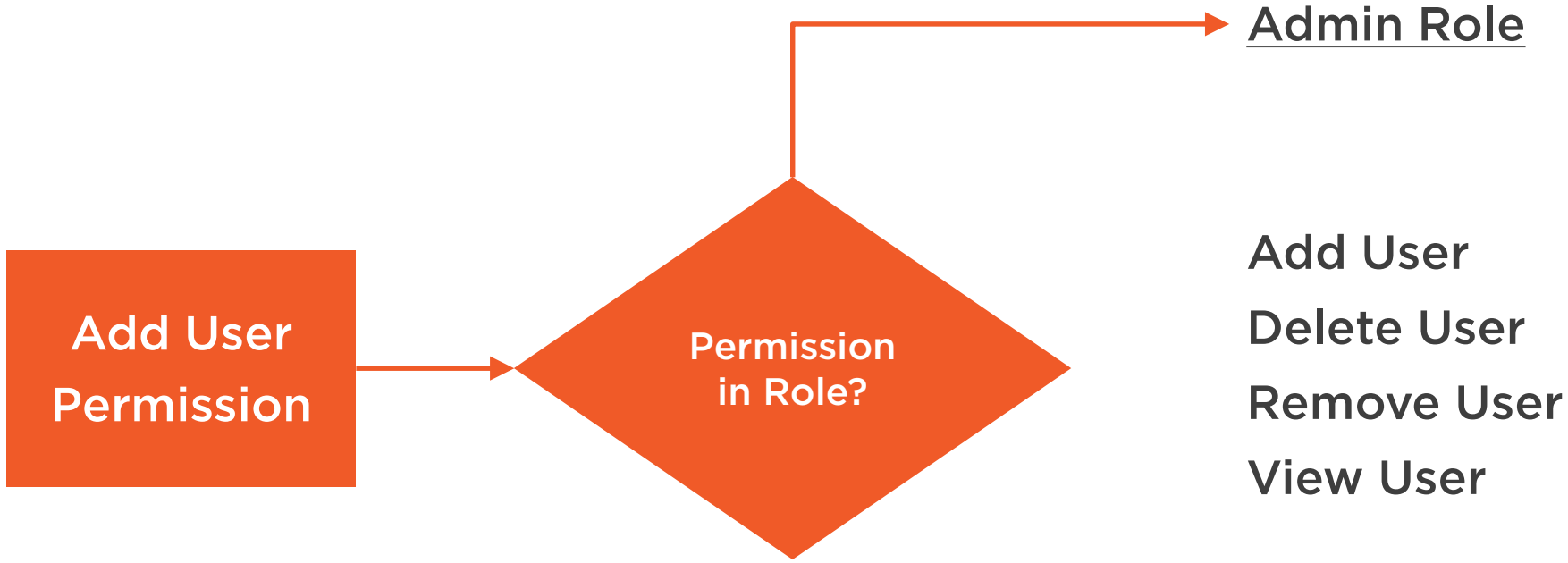
Role Based Access Control (RBAC)



Role Access Control

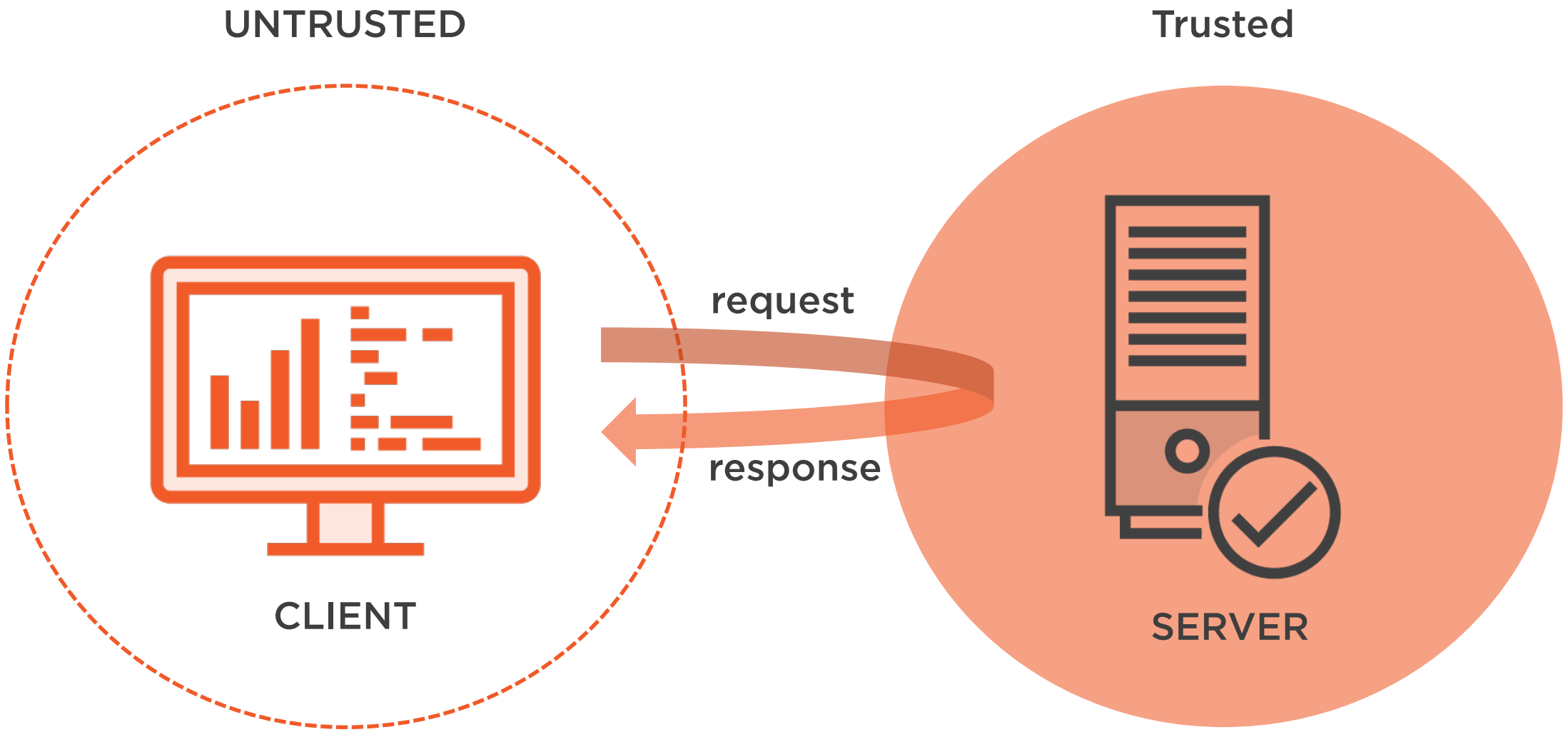


Role Access Control



Server-side Function Level Control Failure

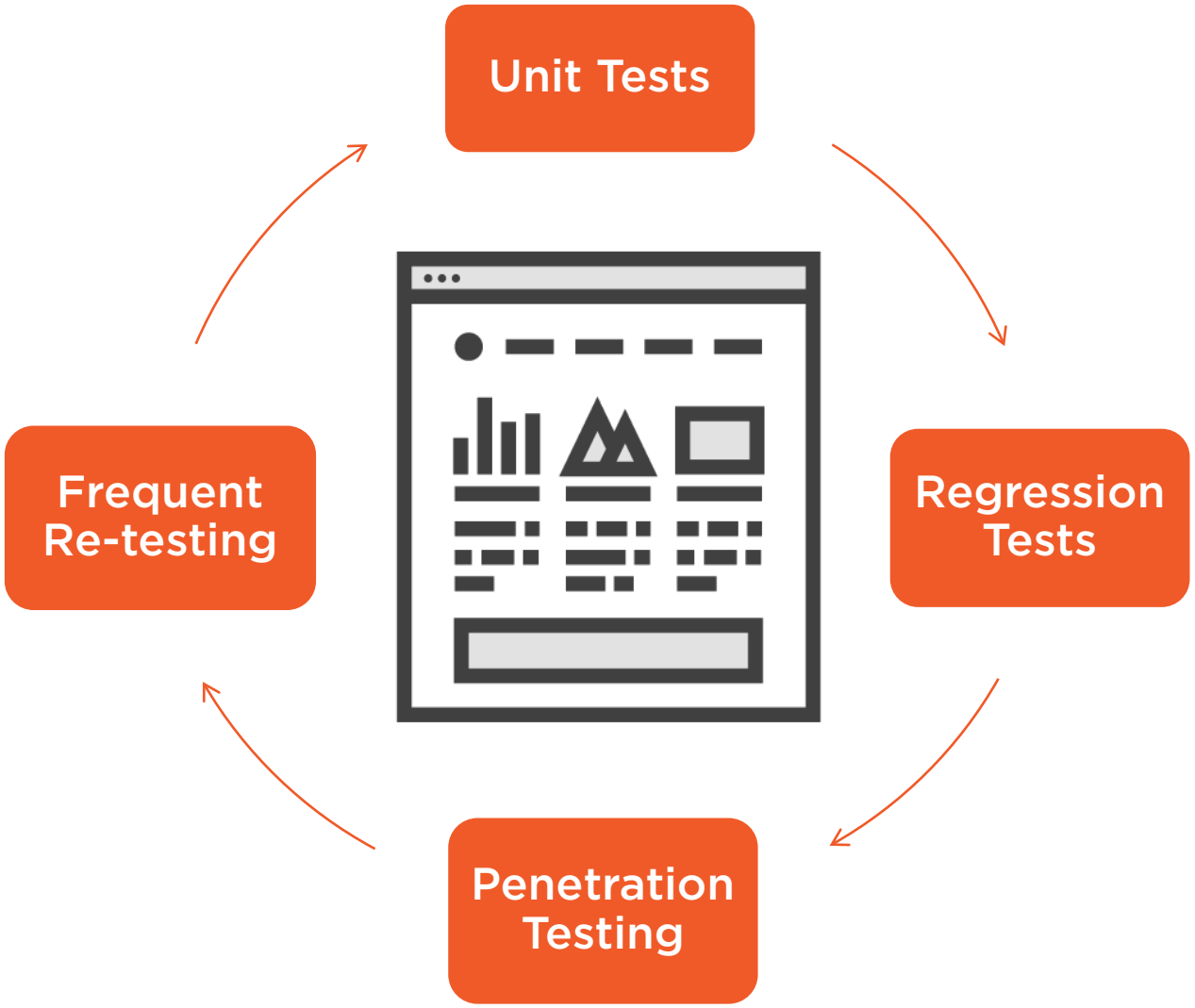
Client Side Validation Only



Server-Side Access Control Validation

All key access control checks and validation must occur on the server-side, despite any client side access control that is conducted.

Access Control Failure Discovery



Summary

- Principle of Least Privilege
- The Problem with Database Access
- Restricting Application Database Access
- Role Based Access Control
- Function Level Controls (with RBAC)
- Server-side Function Level Control Failure
- Access Control Misconfiguration