# The Identity Management Lifecycle

**Kevin Henry CISA, CISSP-ISSMP, SSCP**
Pluralsight Author

kevin@kmhenrymanagement.com

# Course Introduction

## Access Controls

- Access Control Concepts
- The Identity Management Lifecycle

This domain is weighted for 15% of the SSCP examination

# Identity Management

Active management of access controls

- Compliance with laws and regulations
- Following best practices
- Establishing accountability

# The Identity Management Lifecycle

**Kevin Henry CISA, CISSP-ISSMP, SSCP**
Pluralsight Author

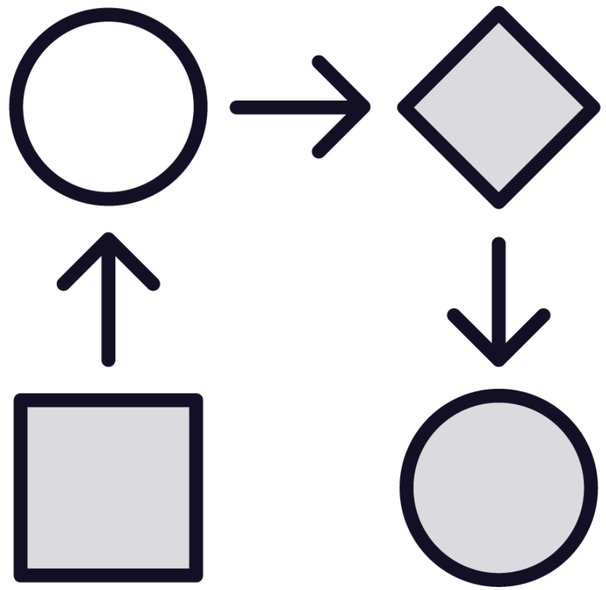
kevin@kmhenrymanagement.com

# Identity and Access Management

**An important responsibility for the Security Practitioner**

- Provision access
- Manage access
- Remove access
- Review access logs
- Provide advice to the System Owner

# Access Management Processes



**Registration**

- Consistent
- Approvals

**Maintenance**

- Changing permissions
  - Privilege creep
  - Privilege escalation

**Revocation**

**Recovery**

# IAM Topic Areas

Identification

Authentication

Authorization

Accounting

# Traceability

Identity and access management manages and tracks all access to systems, assets, buildings, and data including tracking the administrative processes of:

- Provisioning
- Modifications to permissions
- Removal of access

# Identification

# Identification

**Claim of unique identifier**

Account number

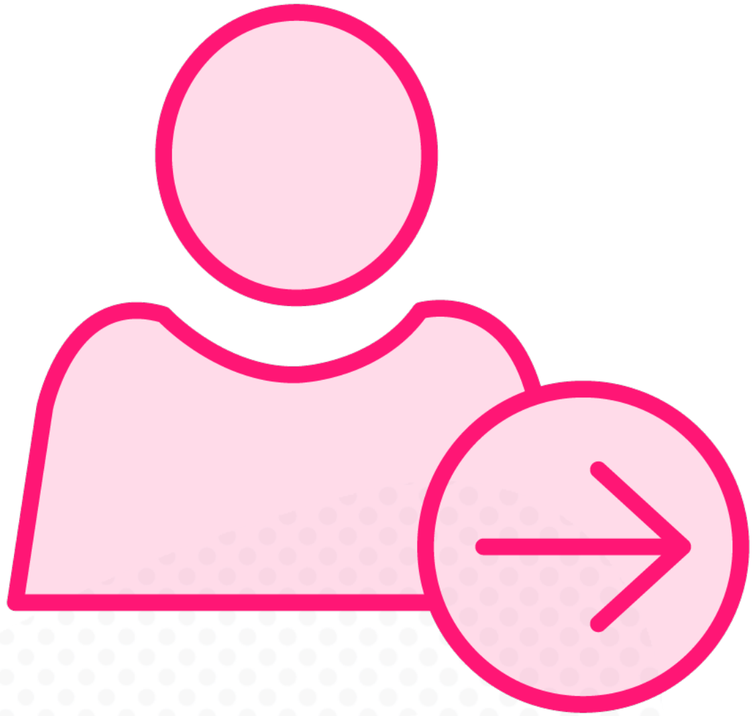
Employee number

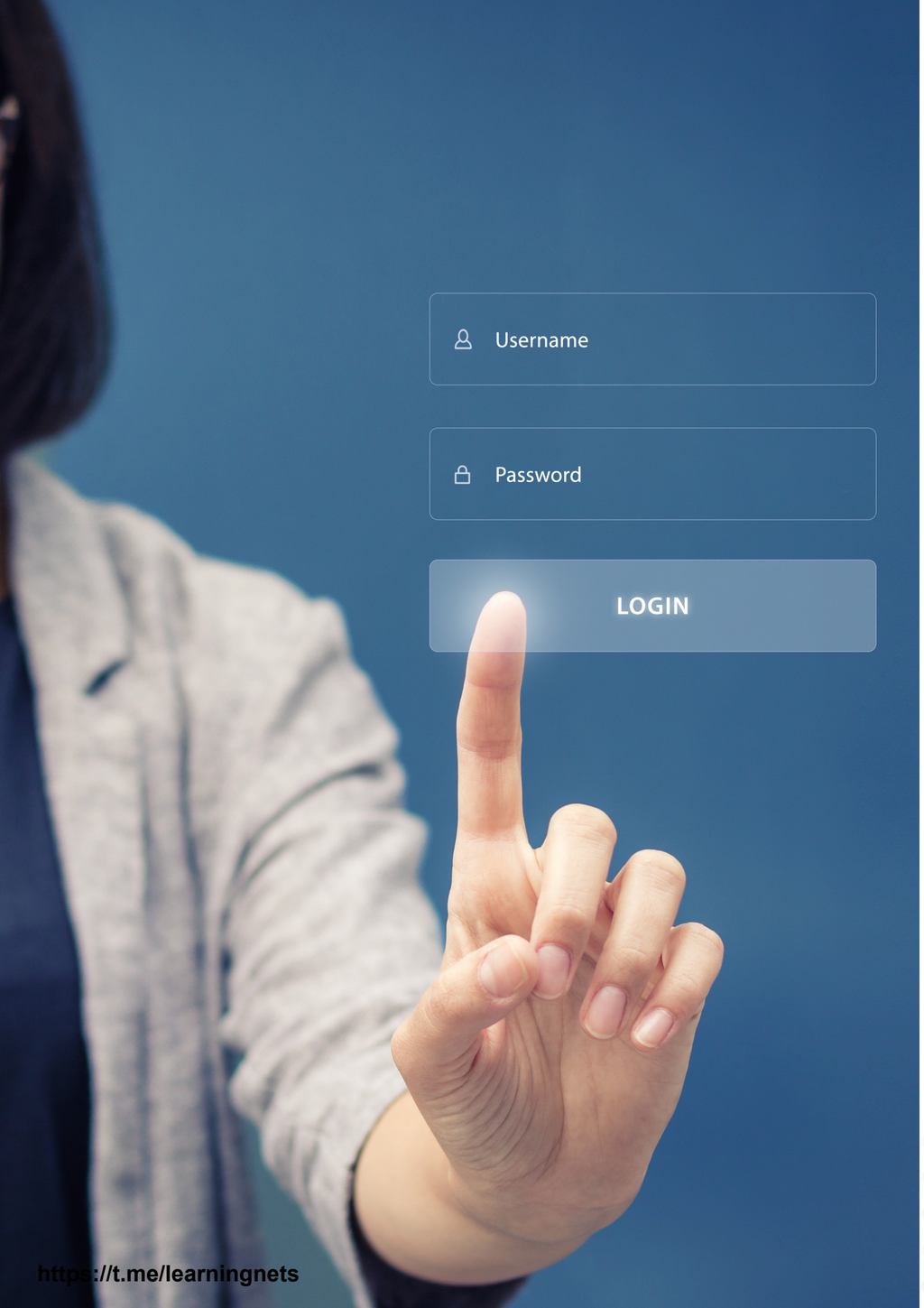
Customer number

Government issued identifier

Email address

User identifier/USER ID






# Proofing of Identity

**Establish ownership of the identity**

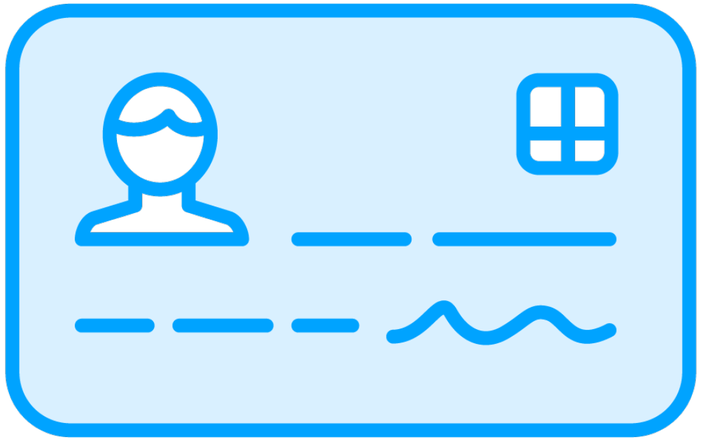
- Secret question

**Password resets**

**Modification to permissions**

**Renewal of certificates**

# Identification



Unique (enables accountability)

Not shared (especially admins)

Secure registration process

- CAPTCHA
- Approval

# Key Points Review

Compliance with regulations, and the ability to conduct an investigation, requires the ability to associate all activity with a defined, unique identity

# Access Management

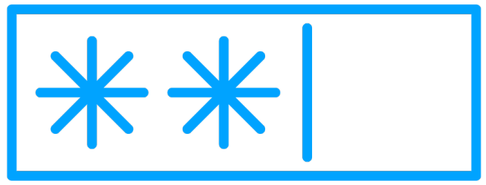
# Management of IAM

**Changes in Technology and Standards**

**Periodic review of access permissions**

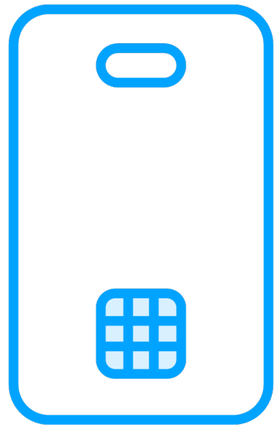
- Changes in roles
- New compliance and reporting requirements
- Removal of inactive accounts
- Association of identity with human resources
  - Contractors
  - Temporary workers

# Access Challenges



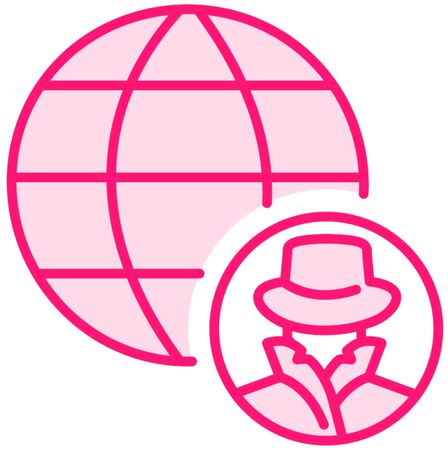
Shoulder surfing
Change passwords
One-time passwords

Screen
lockout / timeout

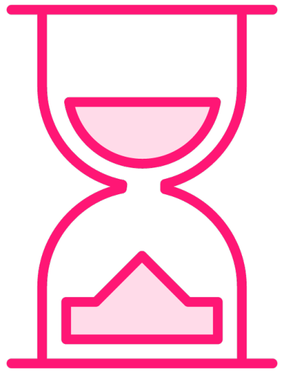


Card readers
Maintenance
Lost cards

# Session Management



Session high-jacking



Timeouts

Periodic or continuous authentication

# Physical Access Controls

**Employee versus visitor parking**

- Parking pass

**Employee versus Visitor entrance**

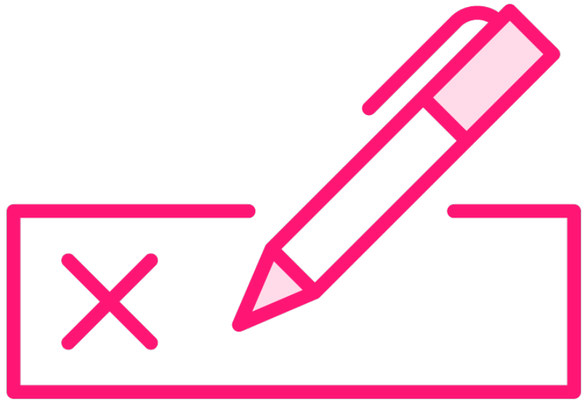
**Escort requirements**

**Temporary pass**

- Requirements to display
- Requirement to return at end of day

# Authentication and Authorization

# Authentication



**Verify, validate, prove the Identity**

- Proof of possession
- Secret question

**What you:**

- Know
- Have
- Are

# What You Know

**Password, passphrase, secret question**

- Static value
- Subject to replay attack
- Should be changed on a periodic basis

# What You Have

**Employee ID badge**

**Token**

**Smartcard**

- Dynamic, one-time password

**Synchronous, asynchronous**

- Time or event
- Challenge Response

# What You Are

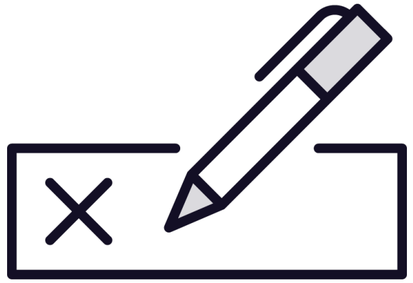
## Biometrics

### Behavioral

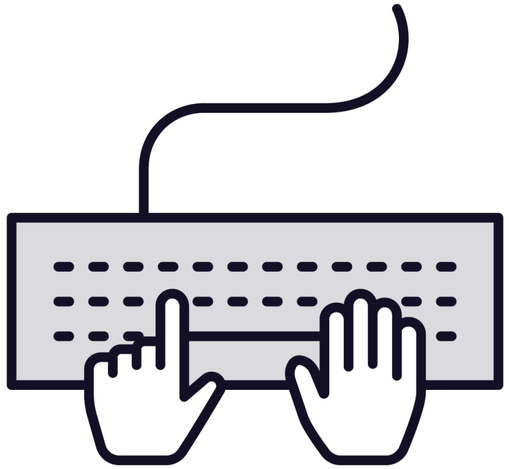
### Physiological

# Behavioral Biometrics

Voice print



Signature dynamics

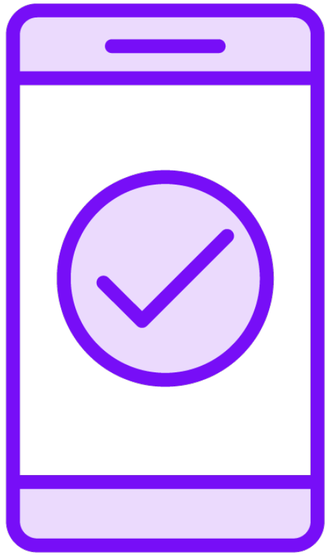


Keystroke dynamics

# Physiological Biometrics

- Iris scan
- Retina scan
- Palm print
  - Venous scan
- Fingerprint
- Facial recognition

# Biometric Acceptance



**User concerns**

- Privacy
- Cleanliness
- Delay in processing

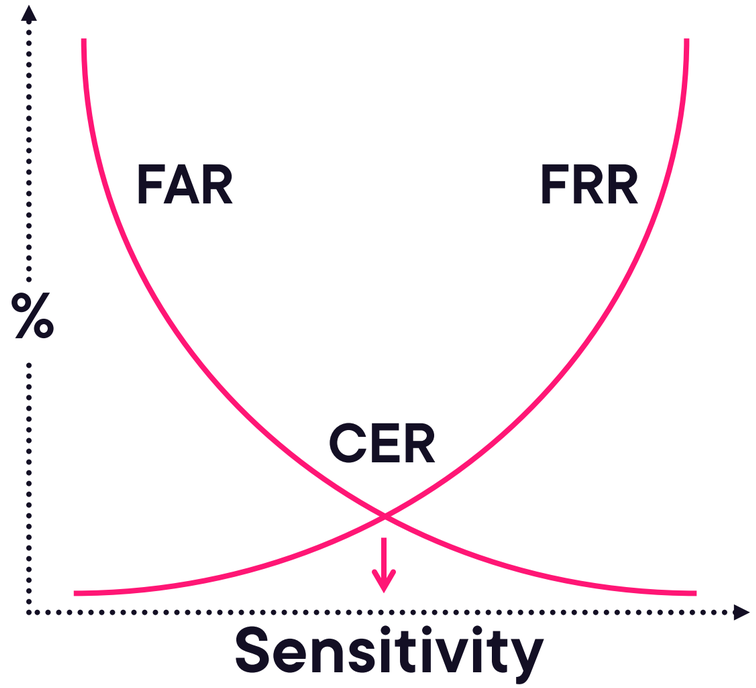
**Cost**

**Maintenance/registration**

# Types of Biometric Errors

**Type 1 error**
**(false reject rate, FRR)**

**Type 2 error**
**(false acceptance rate, FAR)**



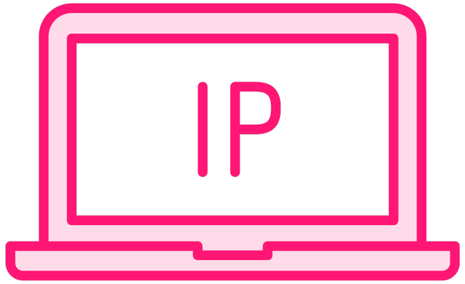

**Crossover error rate**

# Multi-factor Authentication (MFA)

Two or three authentication factors

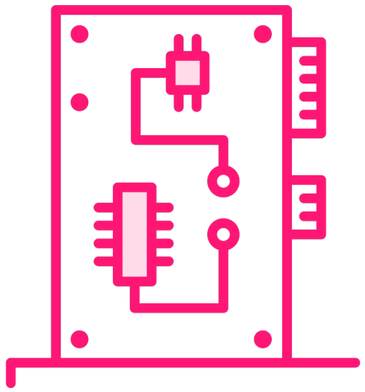
# Node Authentication

## Authentication based on device:




**IP address**
**Certificates**


**RFID**
Radio frequency identification



**MAC address**
**Trusted Platform Module (TPM)**

# Key Points Review

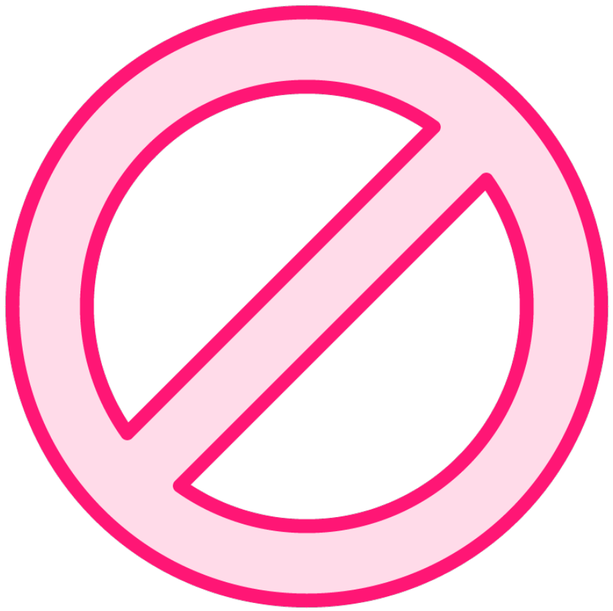
Authentication verifies that only the rightful owner of an identity is able to use that identity

# Authorization

# Authorization

- Rights
- Privileges
- Permissions
- Granted to an authenticated entity

# Examples of Permissions



**Read, write, update**

**Execute, create, delete**

**Least privilege**

**Need to know**

**Separation of duties**

- Dual control, mutual exclusivity

# Accounting/Auditing

Tracking and logging all activity on a system

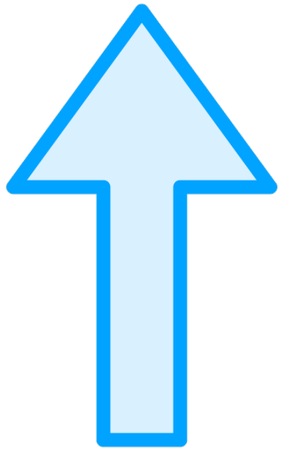
Associate all activity with an identified user or process

Log retention

Regulatory

Business needs

# Advantages of Single Sign-on (SSO)



**Reduce number of:**

- Logins
  - UserIDs
  - Passwords
  - Time to login

**Centralized management**

# Disadvantages of SSO

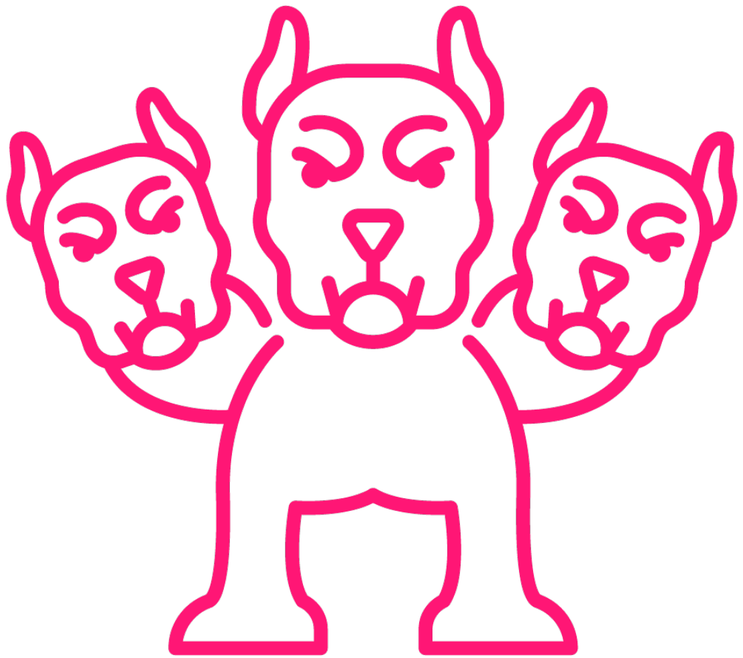
Single point of failure

Requires protection of centralized server

Single point of compromise

Lack of flexibility

# SSO Implementations



Kerberos

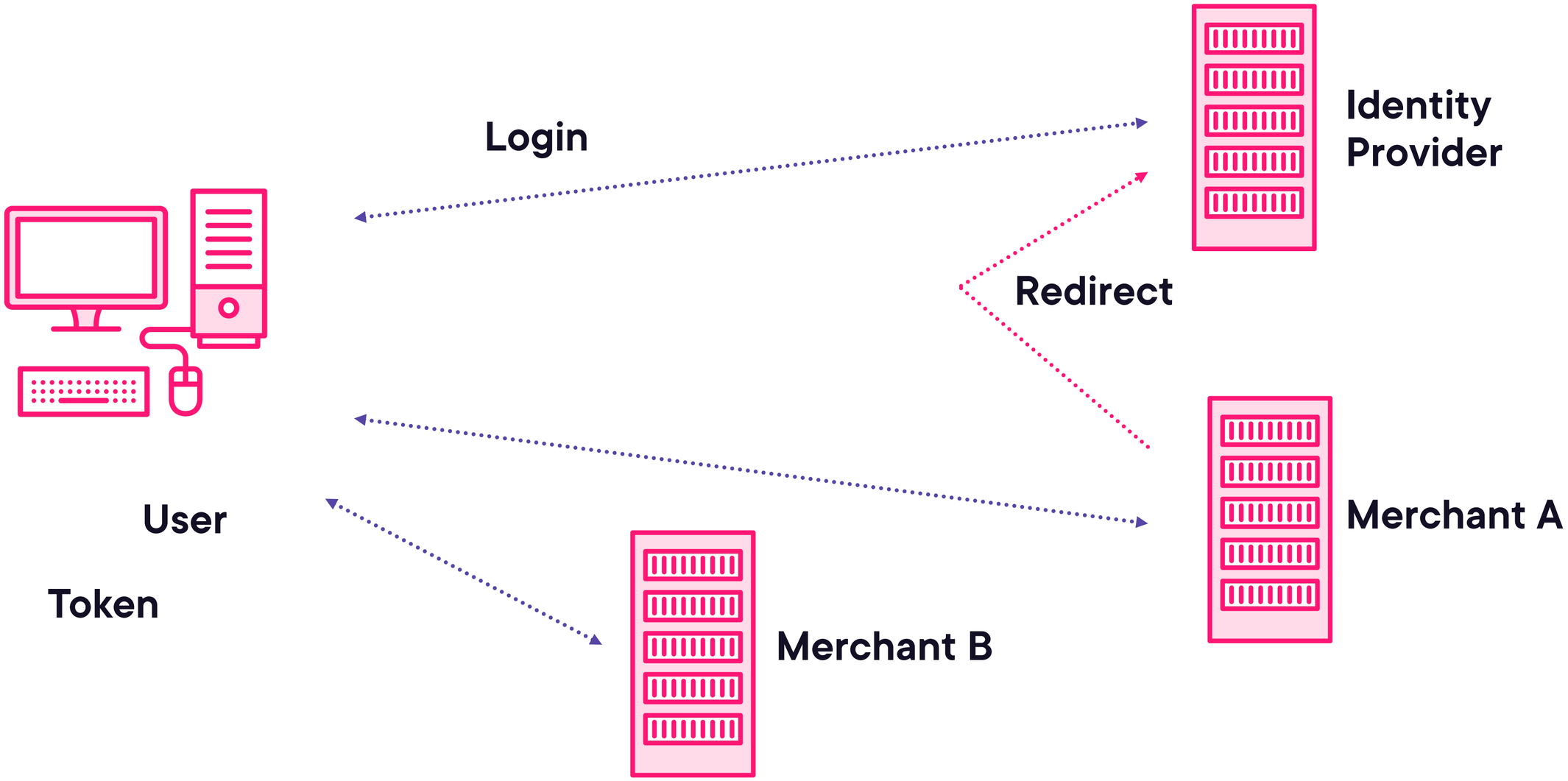
Active Directory Federation Services (ADFS)

OpenID Connect

Open Authorization (OAUTH2)

Security Assertion Markup Language (SAML)

# Federated Identity Management



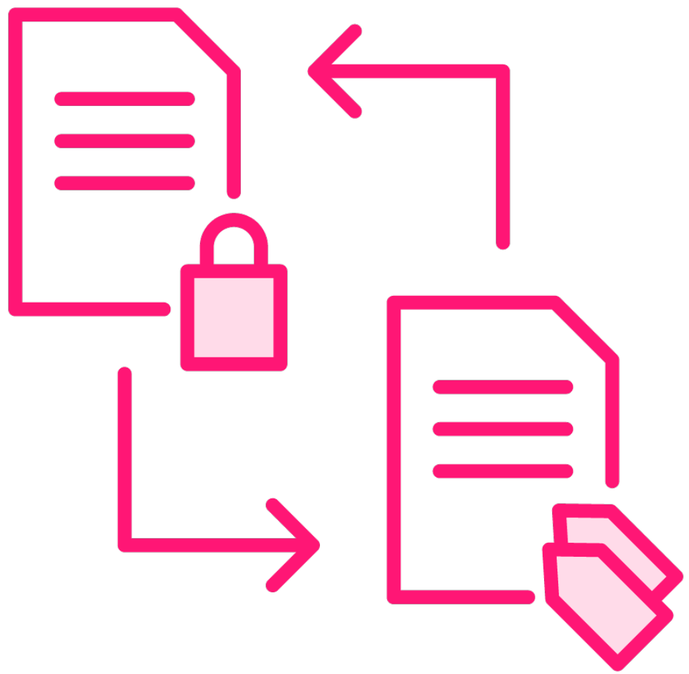
# Key Points Review

**The challenges of managing access have been addressed through many different solutions – but the principles remain the same:**

- Have policy
- Train staff
- Follow procedures
- Perform regular reviews and audits

# Network Trust Architectures

# Zero Trust Architecture



**Defenses move from static, network-based perimeters to focus on users, assets, and resources.**

**The principle of no implicit trust granted to users or user accounts based on physical or network location**

**Response to the challenge of:**

- Remote users
- BYOD
- Cloud-based assets

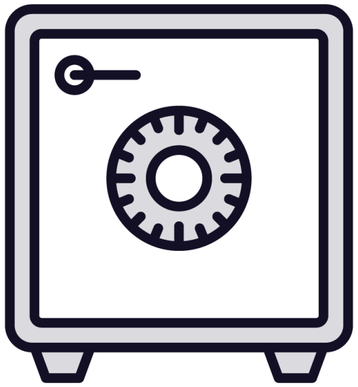
csrc.nist.gov/publications/detail/sp800-207/final

# Zero Trust

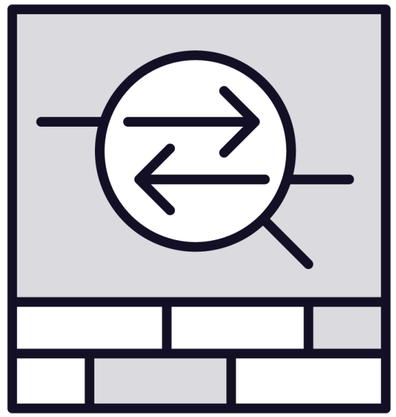
Authentication and authorization (both subject and device) are discrete functions performed before a session to an enterprise resource is established

csrc.nist.gov/publications/detail/sp800-207/final

# Goals



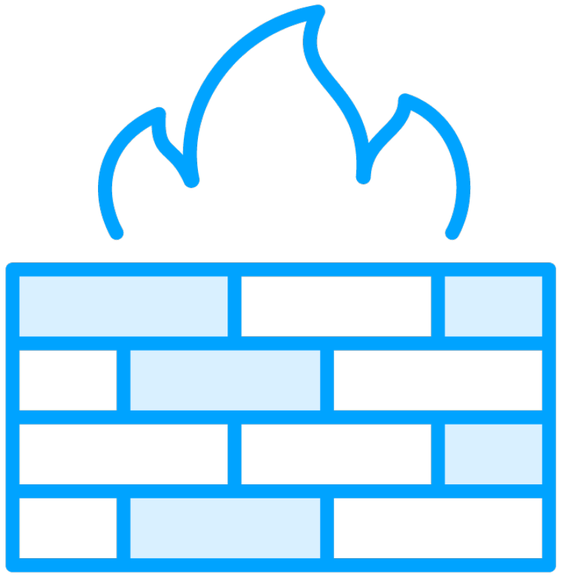
Protect data assets



Prevent lateral movement

Continually authenticating

# Trusted Internet Connections



**Firewalls**

- Protect inbound attacks
- Not effective against internal attacks if only located at the perimeter
- Cannot protect devices and users outside of the network

# Concept

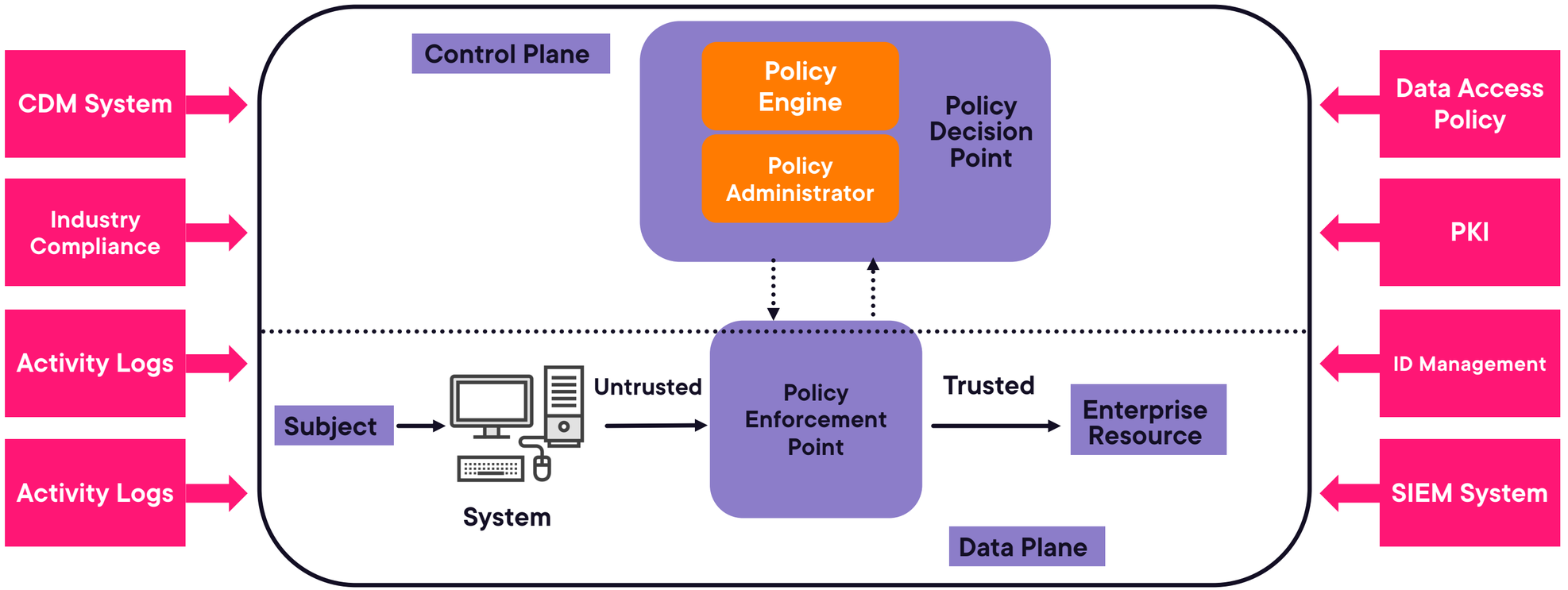
Enforce least privilege per request

Make access control as granular as possible

Monitor, measure, and provide dynamic policy enforcement

Secure all communications regardless of network location

# Zero Trust Architecture




NIST.SP.800-207-pdf page 9

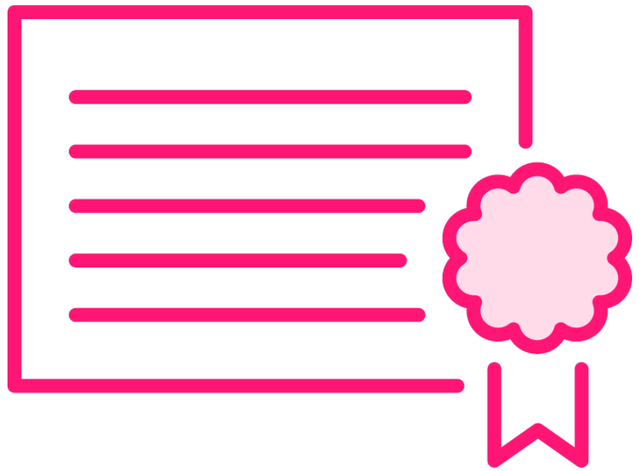
CDM – Continuous Diagnostics and Mitigation

# Key Points Review

The core concept of Zero trust is ‘trust no one’. Verify all access requests and do not be a victim of a TOCTOU attack.

# Trust Relationships

# Trust Relationships



**One-way trust**

- Certificate based
  - Digital signature on a patch
  - Reverse authentication
- Forward authentication
- Node authentication
  - Device MAC
  - Device serial number
    - Data from a sensor

# Trust Relationships

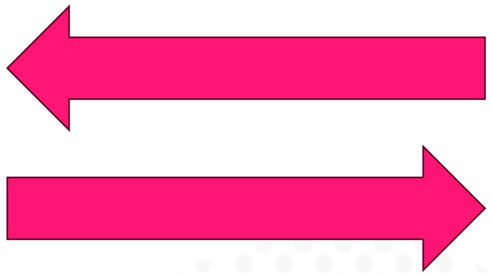
**Two-way trust**

Certificate based

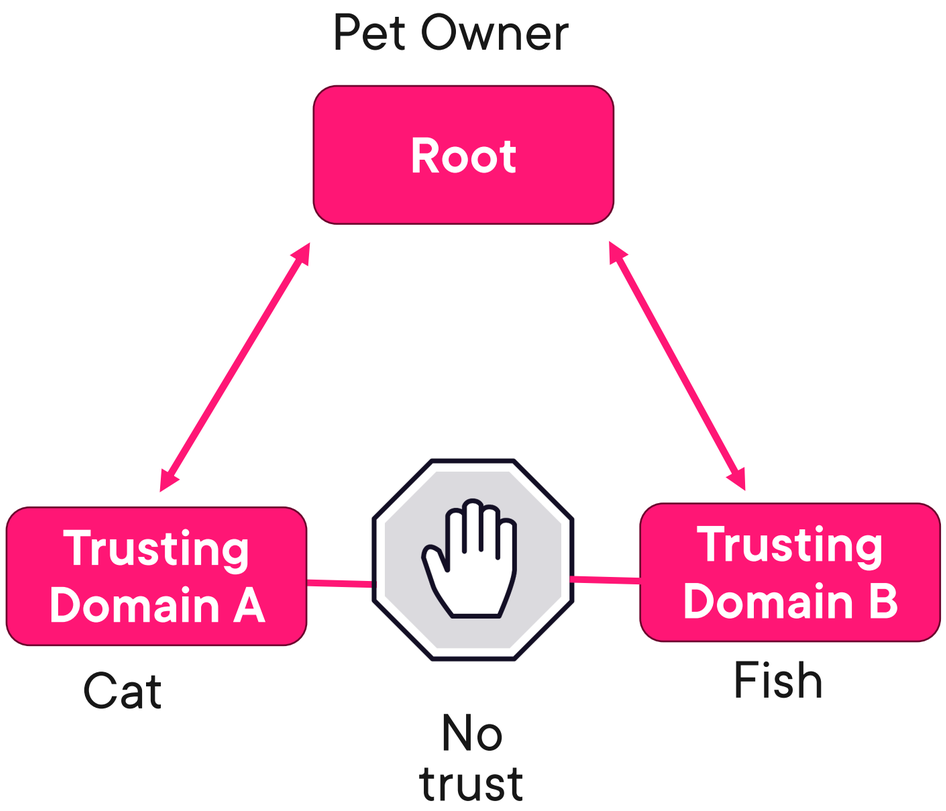
Mutual authentication

Parent child relationships

Peer relationships



# Direction and Transitivity



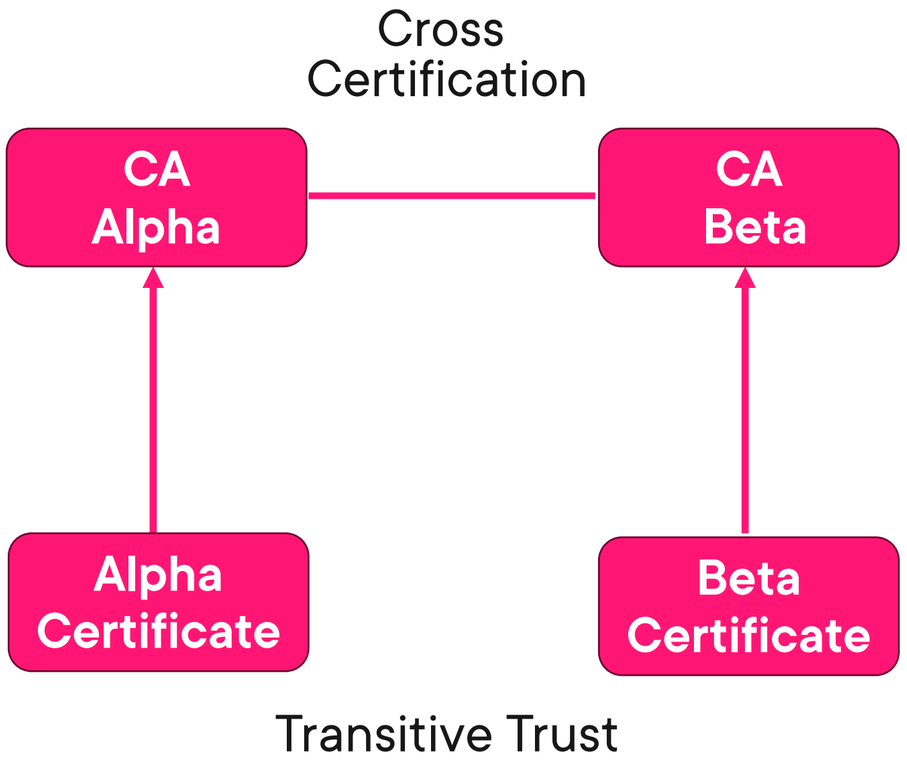

**Rules that govern the flow of information**

**Direction of trust flows from the trusting domain to the trusted domain**

- Everybody trusts root
- But not everyone that trusts root trust each other
- This is an example of two one-way trust relationships

**Direction of access flows from the trusted domain (the owner) to the trusting domain**

# Direction and Transitivity

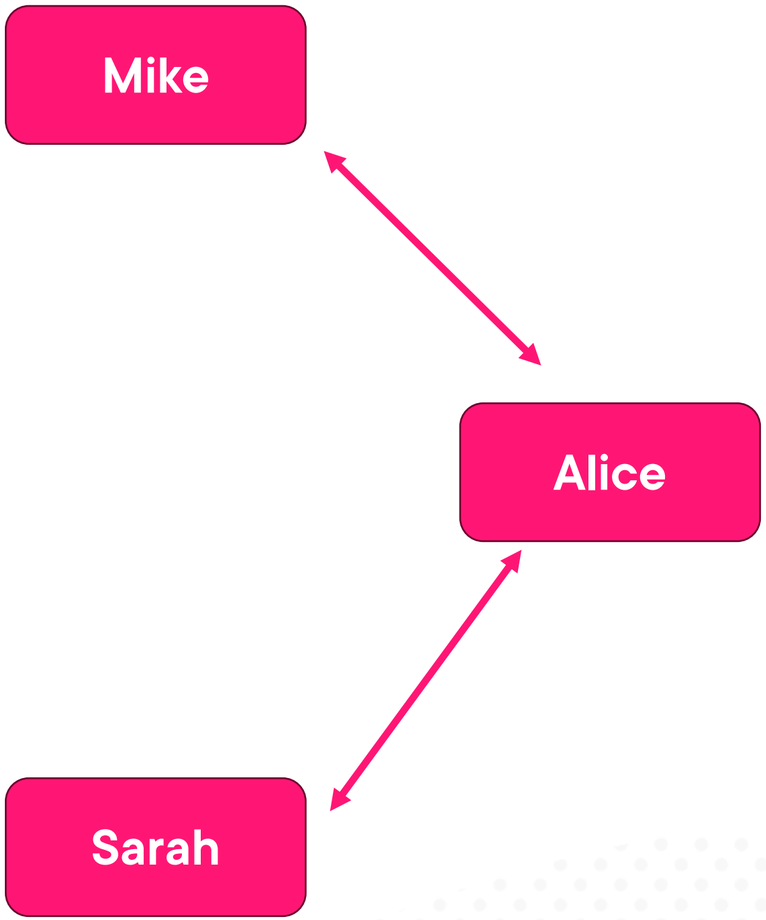



Different Certificate Authorities (CAs) issue certificates to their clients. Each client trusts their own CA, but how can they trust the certificate issued to a client of the other CA?

There needs to be cross certification between the CAs. This establishes transitive trust between the different groups.

This is based on a parent child relationship.

# The Social Media Problem



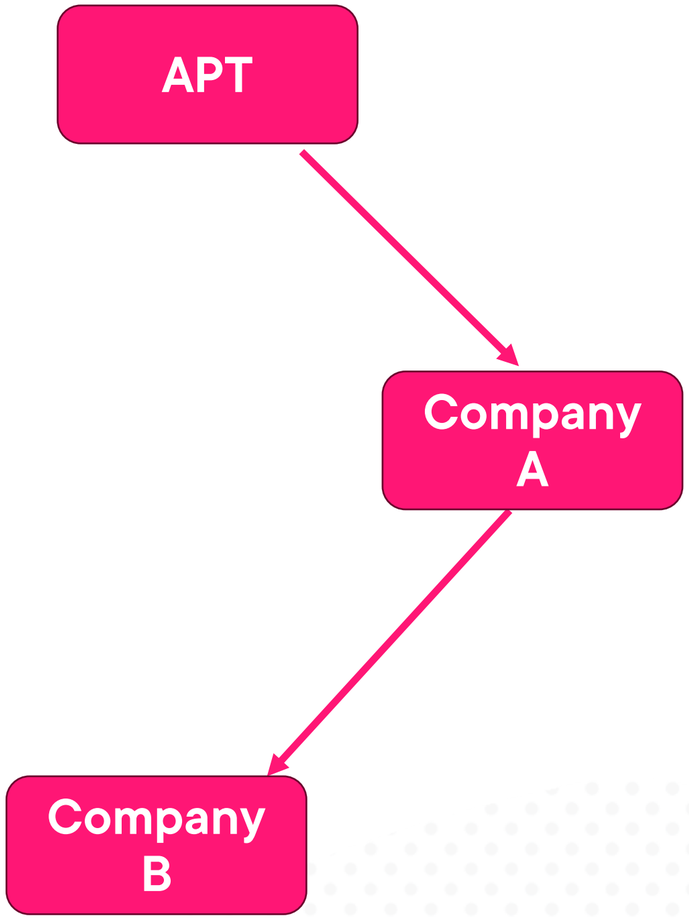

Mike trusts Alice and Alice trusts Sarah. Therefore, can Mike trust Sarah?

What level of trust should exist between the various parties?

What if one of the members of the trust relationship ends up trusting a fake profile?

Access control rules must be written carefully to still provide isolation and protection from improper relationships.

# Chained Exploit




An APT compromised Company A through a phishing attack

Company A had a trusted relationship with Company B

This allowed the APT to compromise Company B

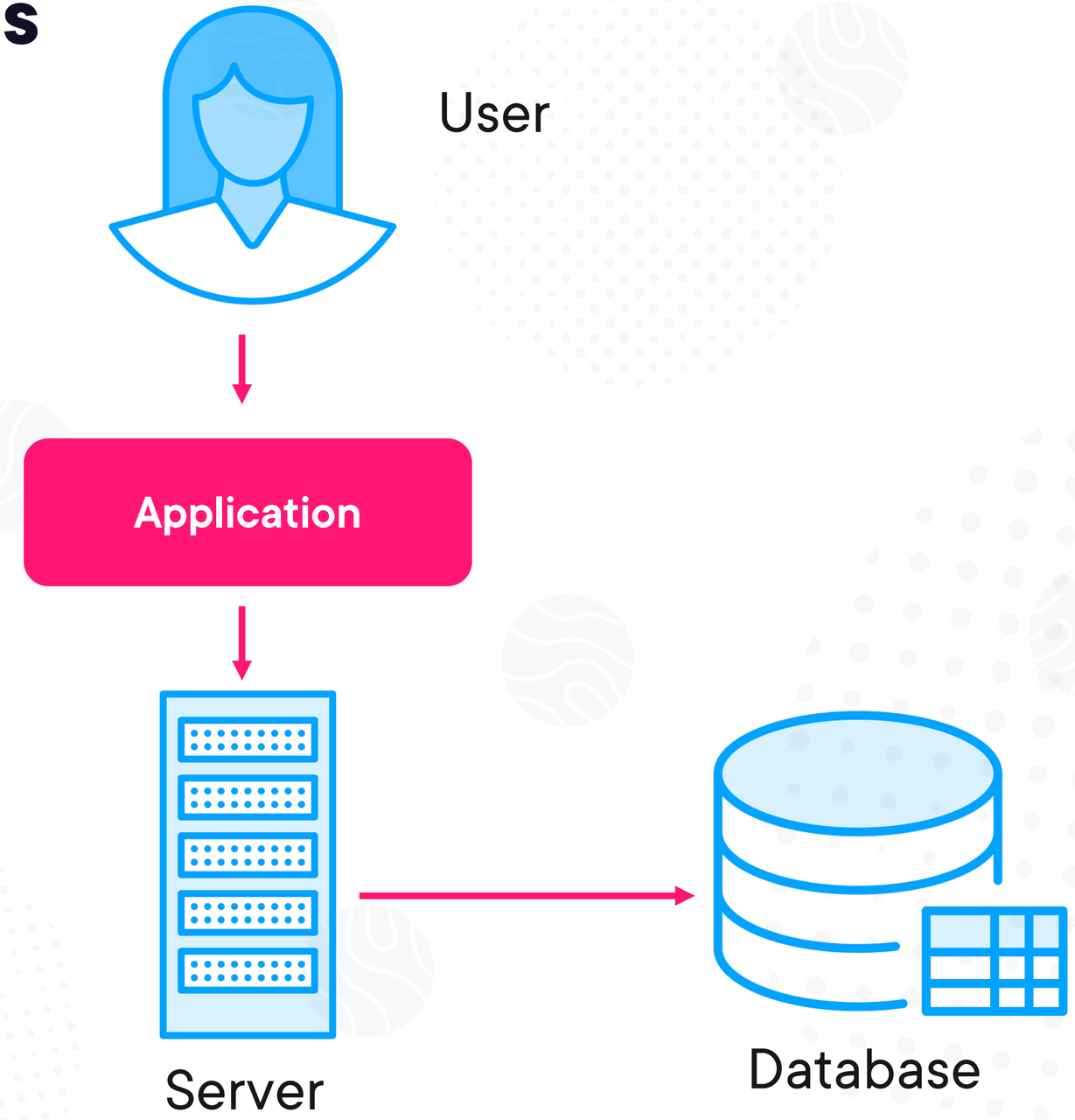
# Key Points Review

**Access Controls are often challenging**

- Many paths to information
- Hidden channels
  - Covert
    - Timing
    - Storage

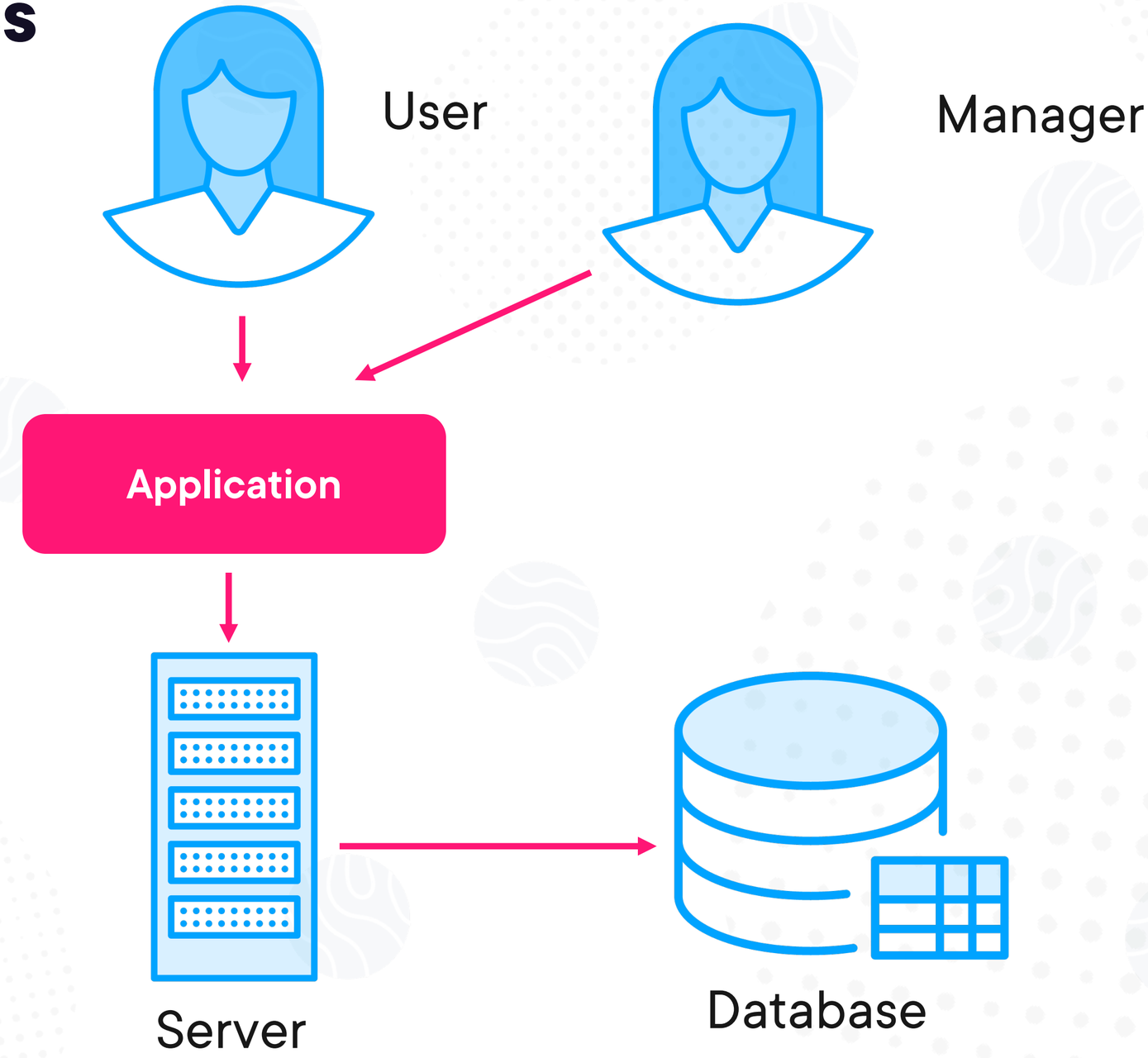
# Internetwork Access

# Application Access Traditional



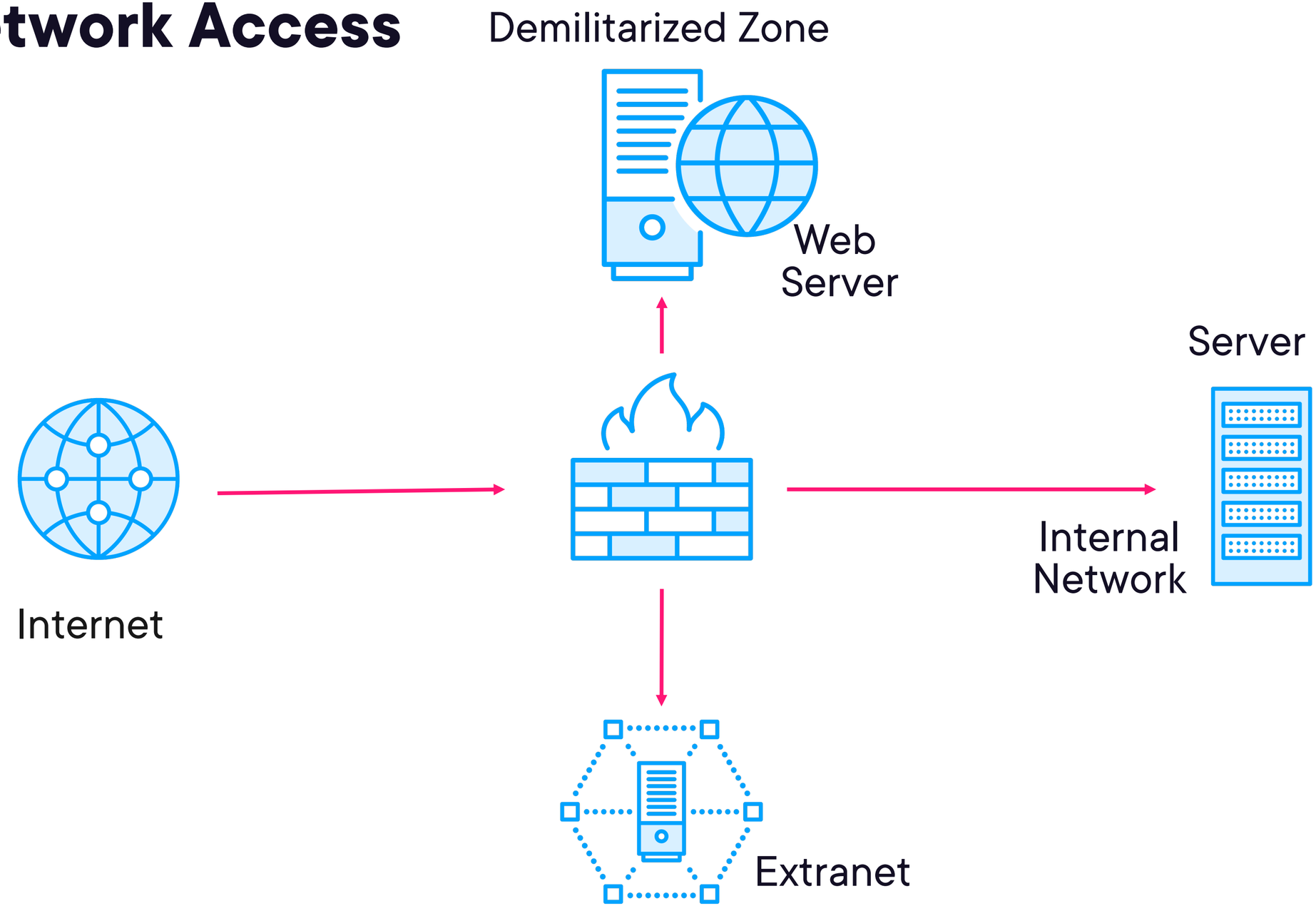

Application access level determined by privilege level of user

# Application Access Traditional

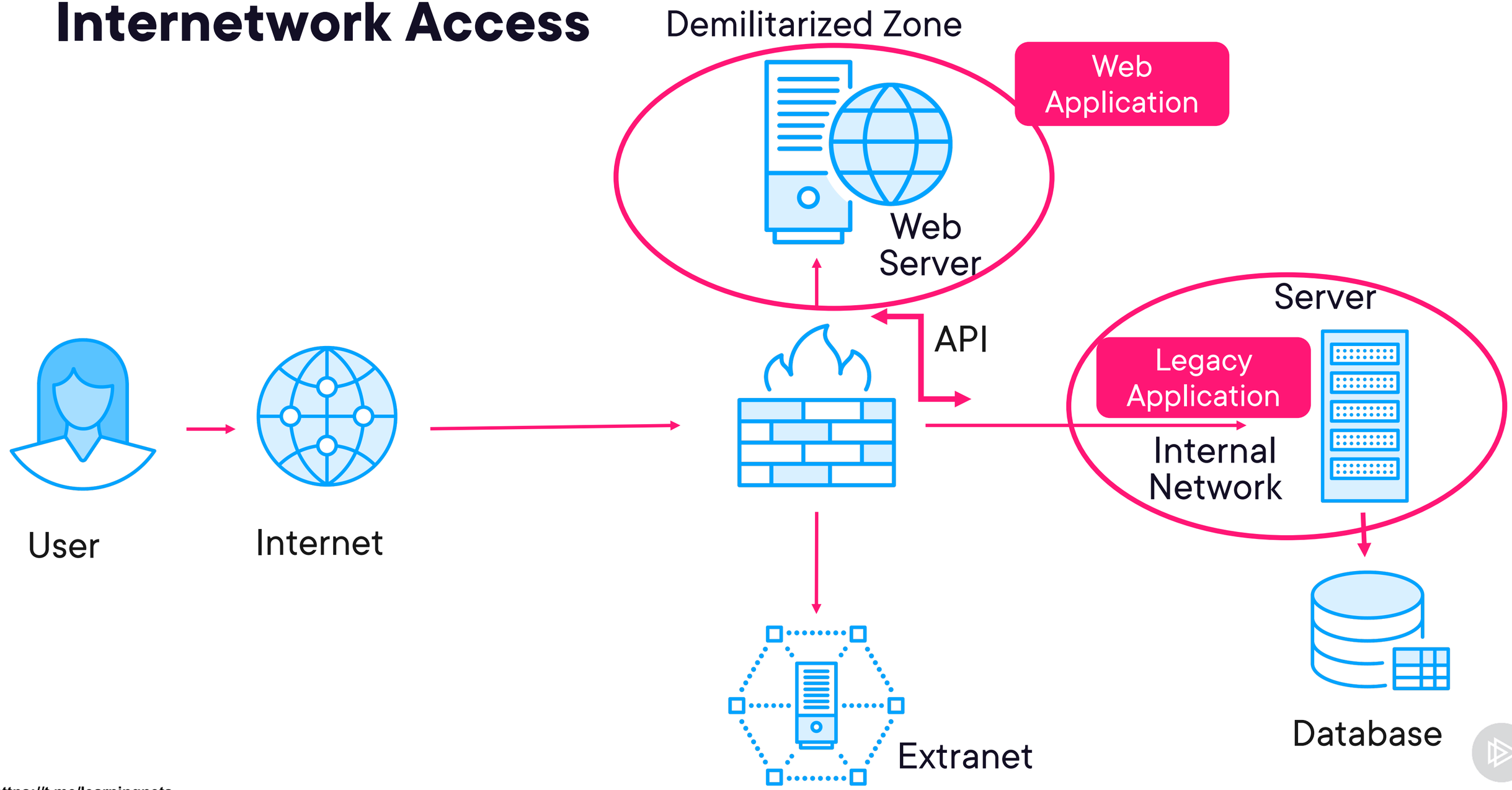



Application access level determined by privilege level of user

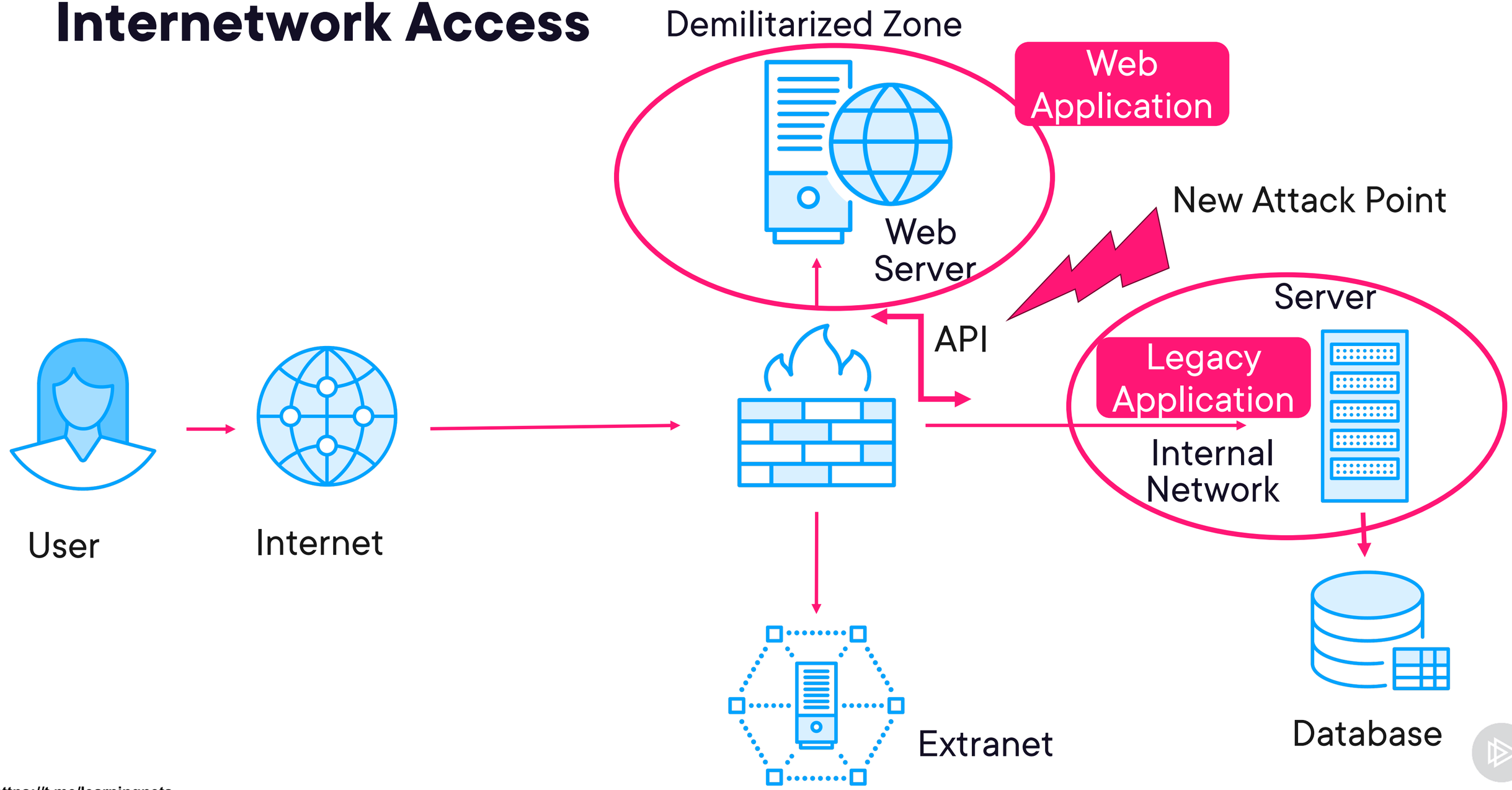
# Internetwork Access



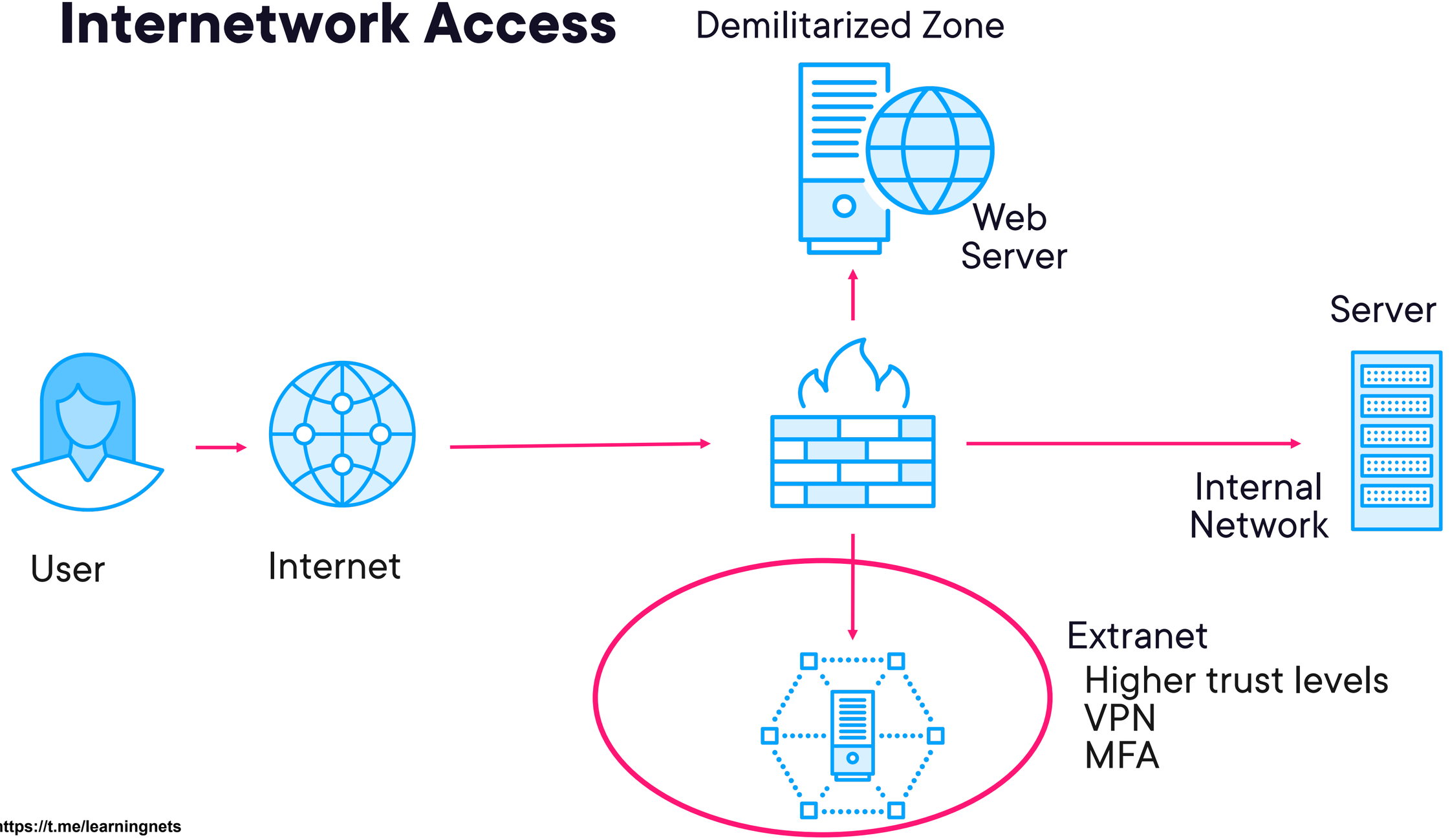
# Internetwork Access



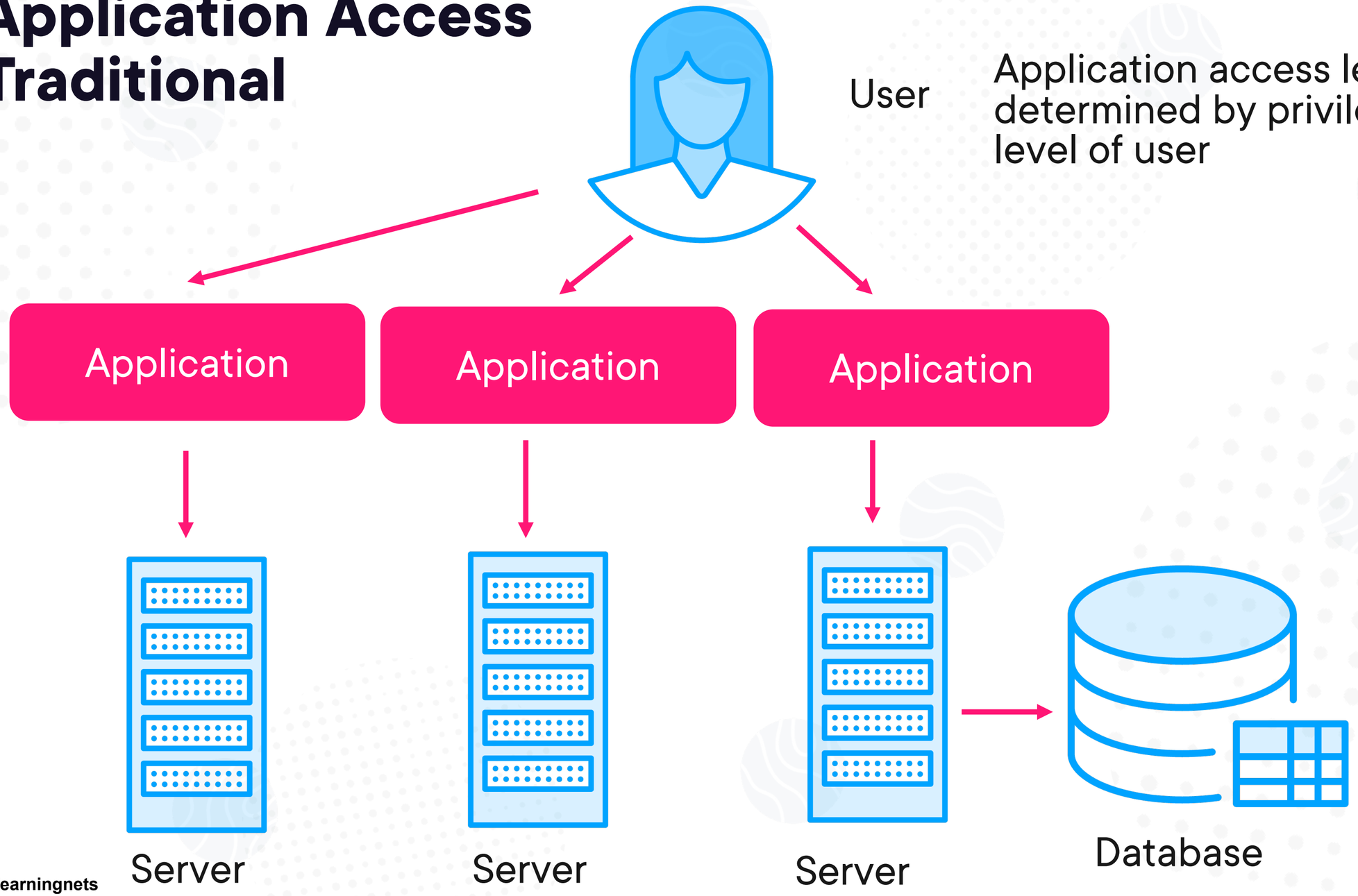
# Internetwork Access



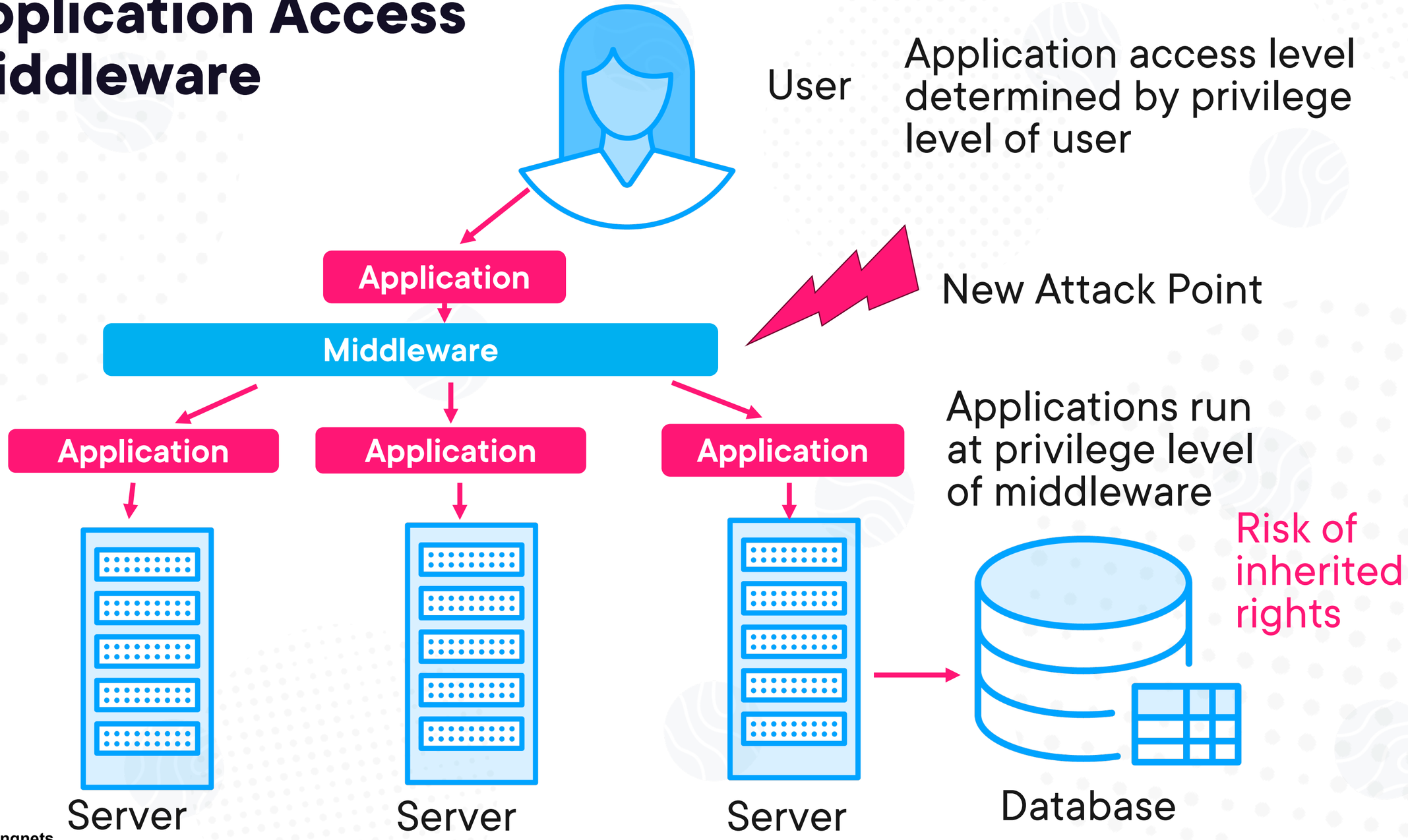
# Internetwork Access



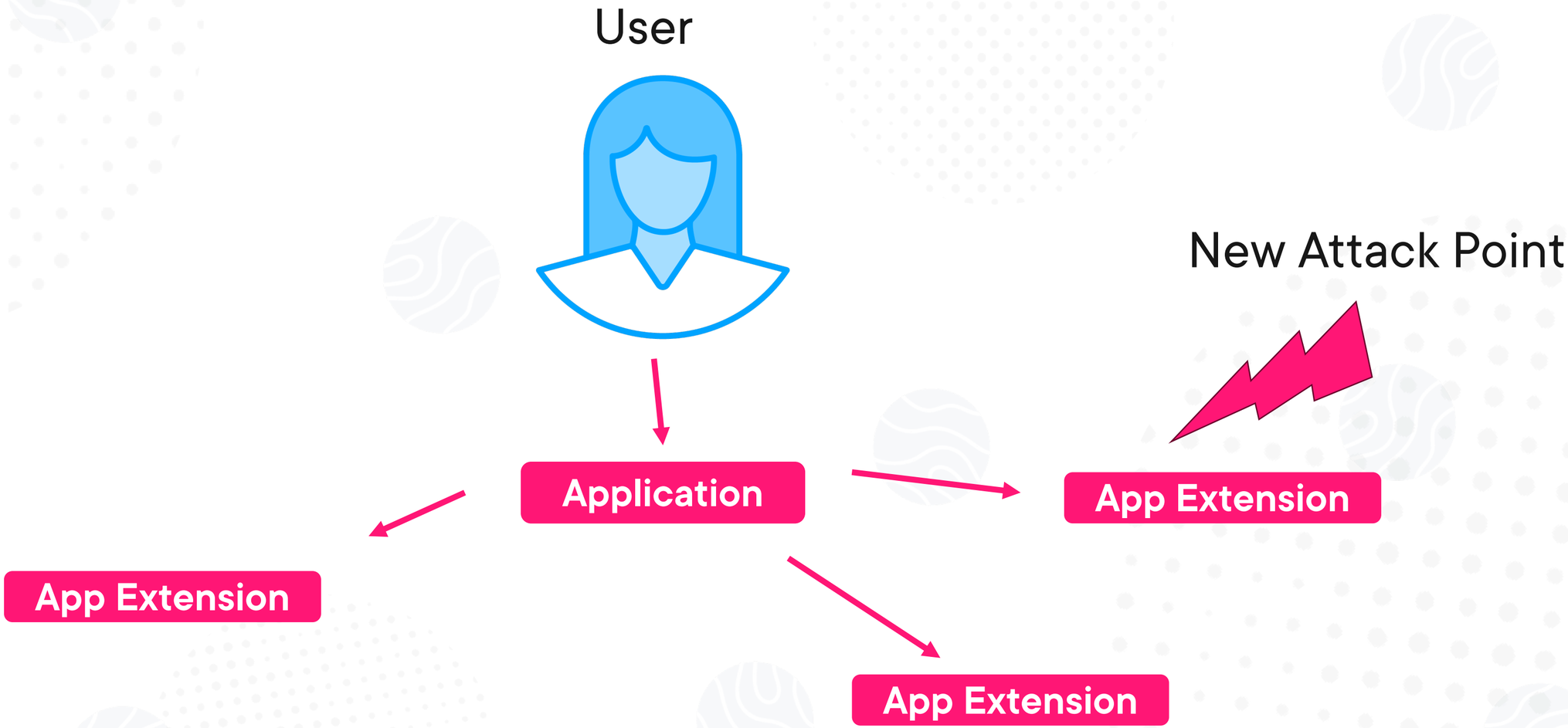
# Application Access Traditional



# Application Access Middleware



# Application Access Controls



# Key Points Review

Application-level access controls present new challenges due to users and internal process threads within the applications having varying levels of access permissions.

Security practitioners must be aware of the risk of privilege escalation.

# Managing External Access

# Good Practice for External Access Controls

- Unique process and user IDs
- Multi-factor authentication
- Architectural separation
- Least privilege

# IoT, ICS, and SCADA Access Risk

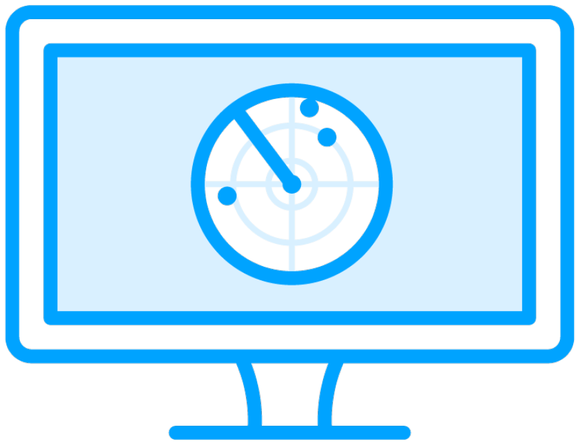
Often connect to internal networks

Often not managed by IT

May not be patched

Benefit from Network Segmentation and Whitelisting

# Remote Access Monitoring



- Audits
- Vulnerability Assessments
- Penetration testing
- Log Review

# Key Points Review

Access control management was much easier when the only users of systems were internal employees!

Now we manage access on a global scale.