



# Identity Access Management

# Sommaire

- **Probleme d'identité aujourd'hui**
- **Identity Access Management**
- **Composants et terminologie**

**ON THE INTERNET**



**NO ONE KNOWS YOUR A DOG**

imgflip.com

- Internet était au départ idéal pour l'anonymat.
- À l'origine, il servait principalement à échanger des articles et travaux de recherche.
- La sécurité n'existe pas encore dans les premières versions du réseau.
- On comptait surtout sur la sécurité **physique** (accès restreint aux machines et aux locaux).
- L'histoire des mots de passe commence avec l'utilisation partagée d'un même ordinateur par plusieurs utilisateurs.



# Identité universelle

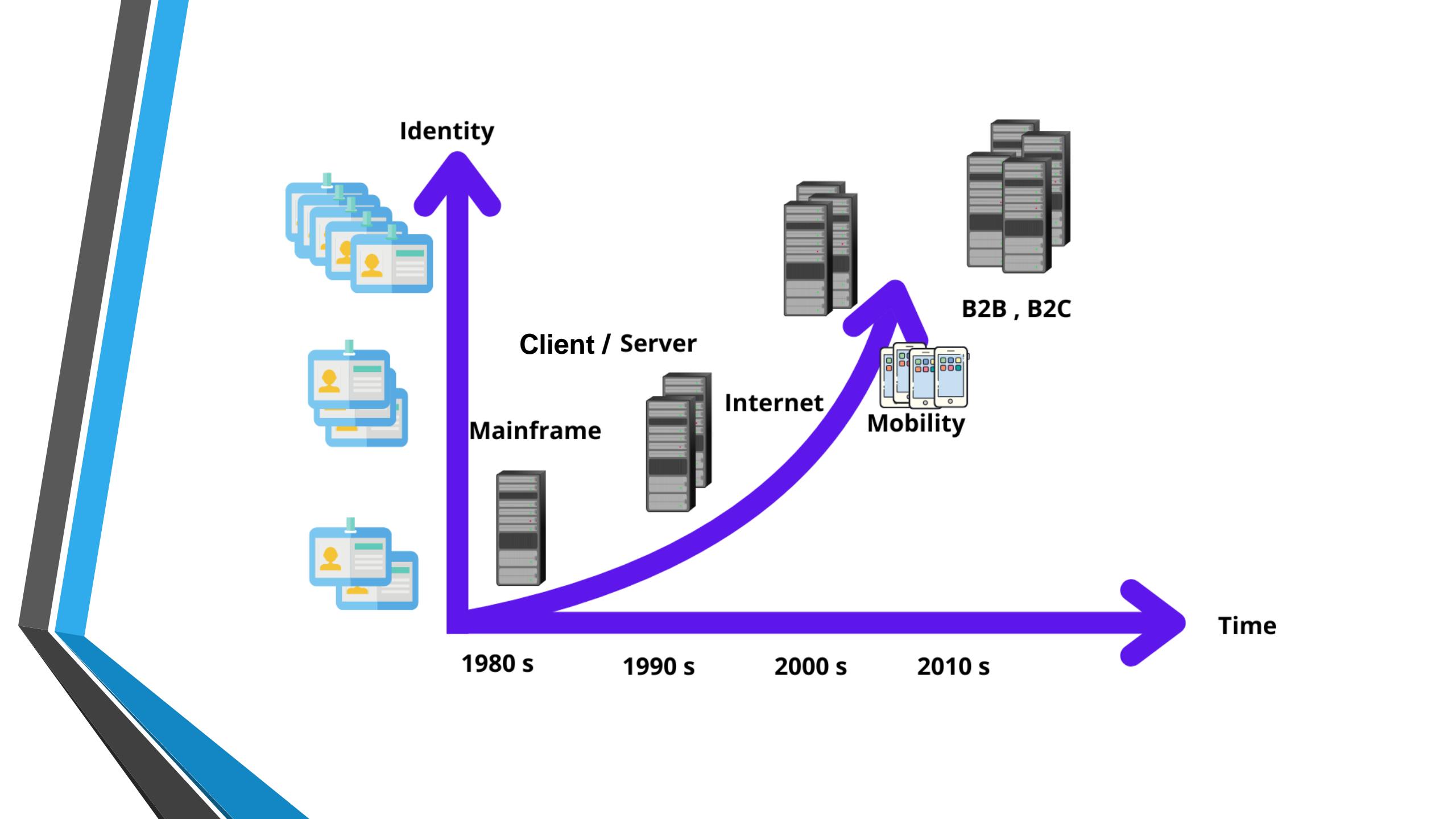
Internet  
Anonyme

Réseau  
Interne

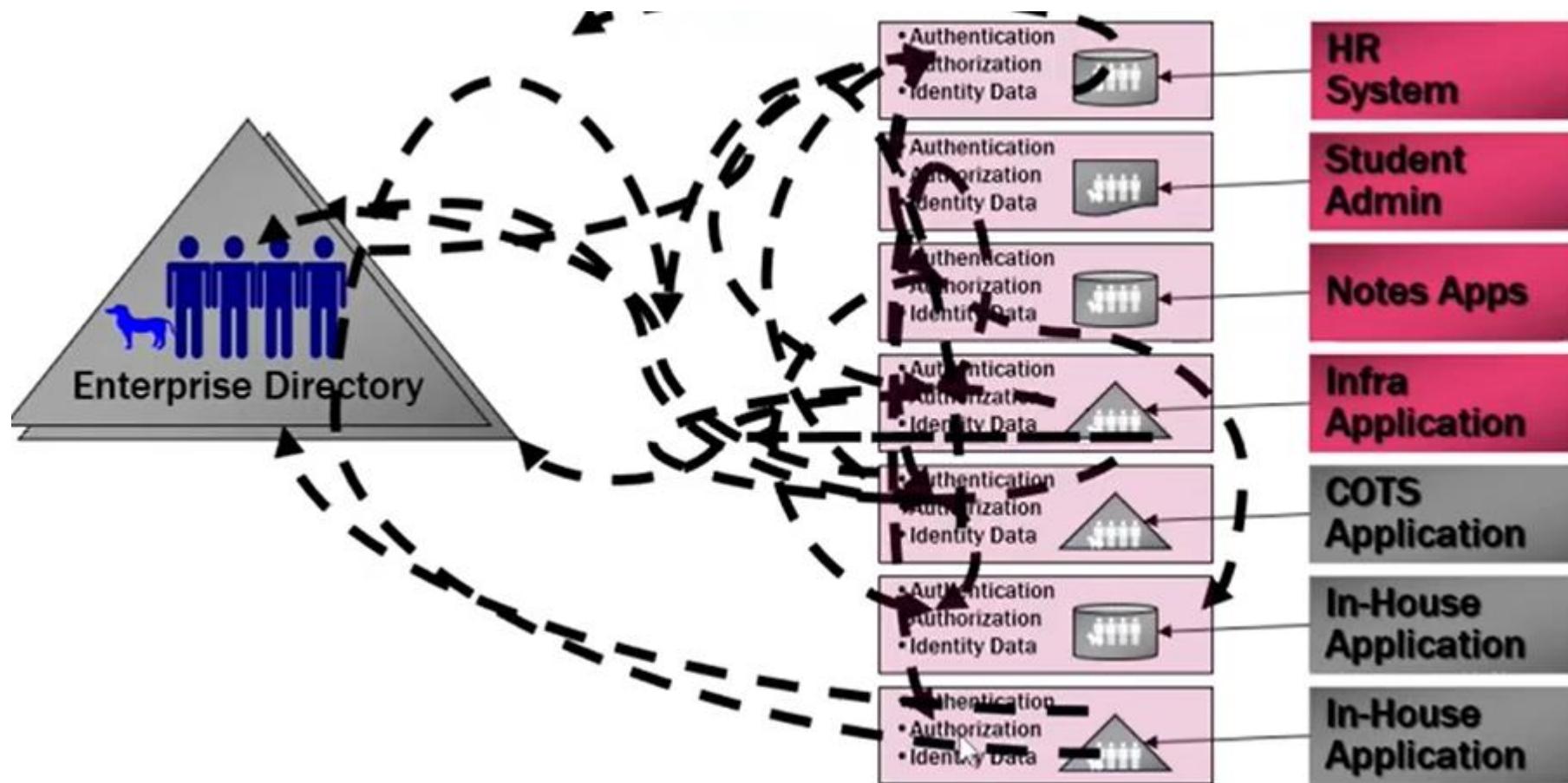
Les  
Utilisateurs

Les  
Criminels

- Dans les réseaux internes des entreprises, il est nécessaire de gérer l'identité des utilisateurs.
- Chaque employé peut avoir plusieurs identités selon les services utilisés (RH, messagerie, différentes applications métiers).
- Cette multiplicité rend la gestion complexe ; la conséquence est souvent l'utilisation du **même identifiant et mot de passe** pour tous les comptes.
- Cela crée une faille de sécurité exploitable par les attaquants.



- Explosion du nombre d'identités numériques.
- Multiplication des applications avec l'émergence du modèle client-serveur.
- Arrivée d'Internet et ouverture vers l'extérieur.
- Dans les entreprises, la notion d'identité s'élargit aux comptes **clients, partenaires, prestataires**, etc.



- Réalité déconnectée entre les différents systèmes.
- Pour accéder à un service, il fallait souvent passer par d'autres services intermédiaires.
- Les employés perdaient beaucoup de temps, ce qui entraînait un coût important pour l'entreprise.

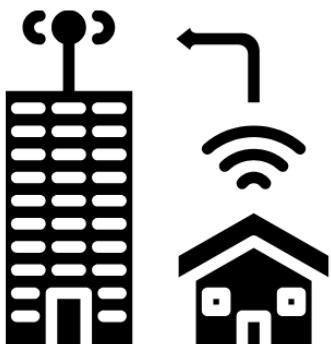
# Le Chaos de l'Identité

- De plus en plus d'utilisateurs et de systèmes à gérer.
- Multiplication des identifications et des mots de passe.
- Gestion décentralisée et complexe des accès.
- La présence de comptes ou d'utilisateurs **orphelins** engendre des problèmes de sécurité.

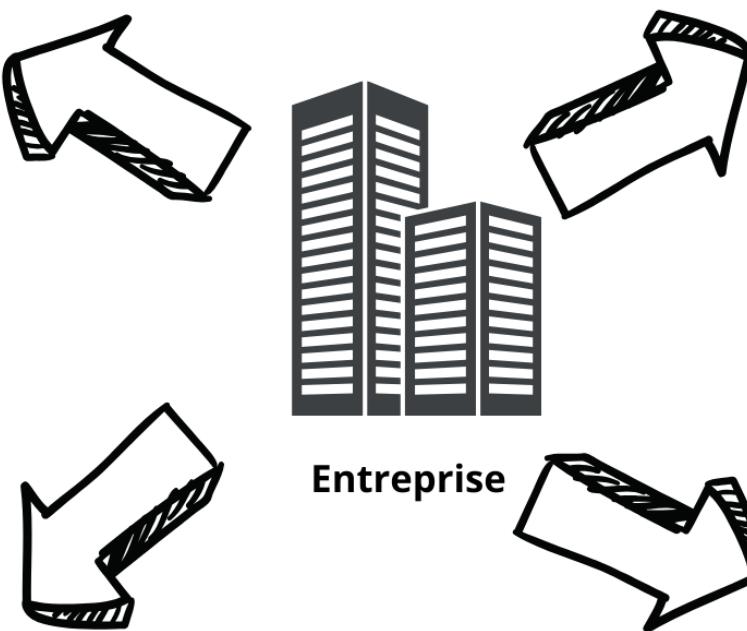
# Context multiple



Clients



Employés à distance



Entreprise



Partenaires



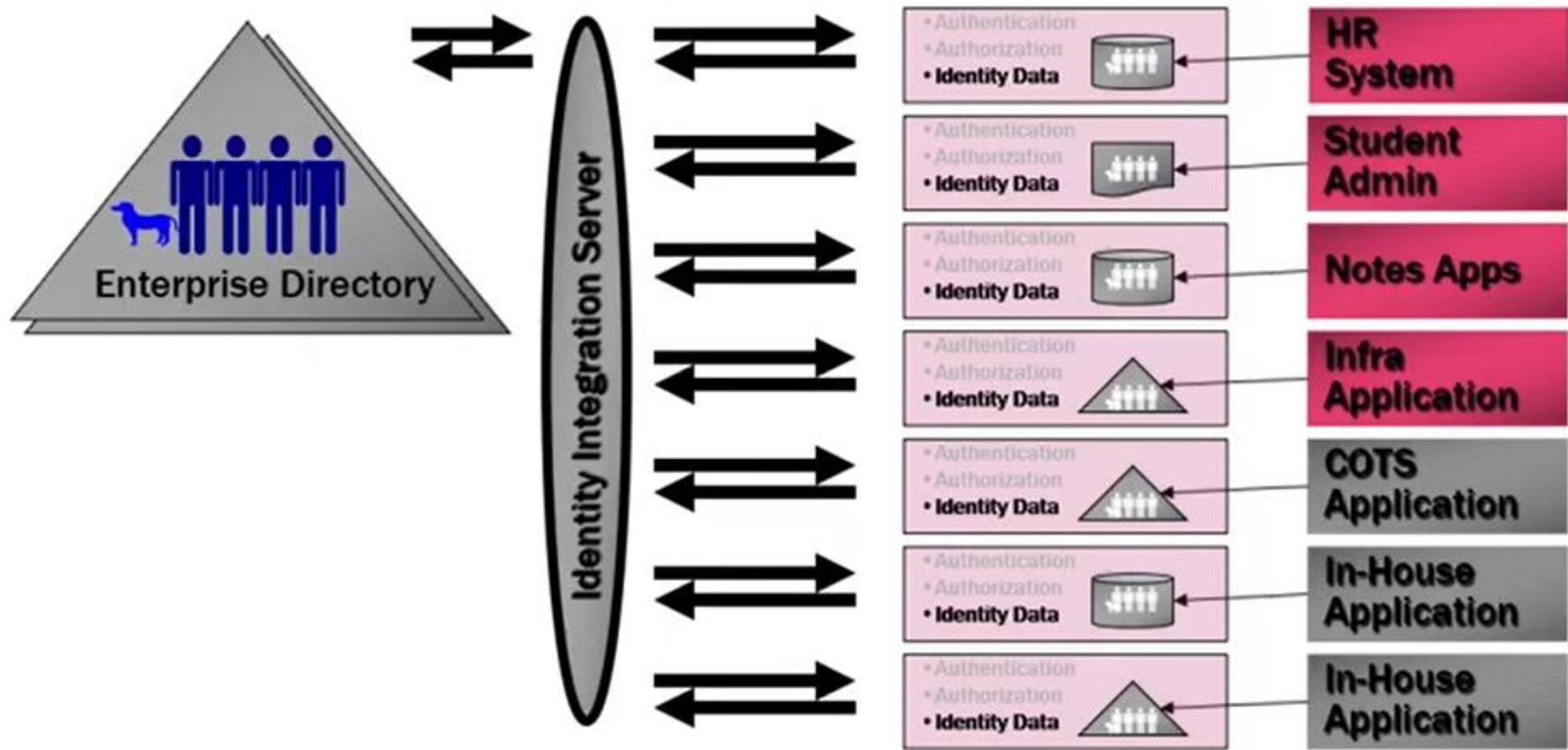
Sous traitants

# Combien d'identités avez-vous?

- Combien d'identités numériques possédez-vous ?
- Combien de temps passez-vous chaque jour à vous connecter à différents services ?
- Combien de mots de passe devez-vous retenir et utiliser ?

## Faire des économies

- Renouvellement obligatoire des mots de passe tous les 3 mois.
- Processus de récupération ou de réinitialisation des mots de passe
- Coût élevé pour l'entreprise, estimé entre **40 et 150 €** par incident.



- **Solution économique** pour l'entreprise et les utilisateurs.
- **Identité centralisée (MFA)** : chaque utilisateur dispose d'un compte unique qui regroupe tous ses accès.
- **SSO (Single Sign-On)** : un seul identifiant et mot de passe permettent d'accéder à **tous les services**, réduisant le temps de connexion et les coûts liés à la gestion des mots de passe.



**IAM**  
**c'est quoi ?**

- Ensemble des processus permettant de **gérer l'accès des utilisateurs**.
- Permet aux utilisateurs d'**accéder aux ressources de l'entreprise**.
- Gestion réalisée de manière **centralisée** pour plus de sécurité et d'efficacité.

# Objectif de l'IAM

-  Confidentialité
-  Conformité
-  Efficacité
-  Gestion des risques

- Les bonnes personnes **accèdent aux bonnes ressources**, au bon moment et pour les bonnes raisons.
- **Contrôle d'accès et surveillance** des actions des utilisateurs.
- Respect des **lois et réglementations**, comme le **RGPD**.
- **Amélioration de la productivité** : le temps perdu pour se connecter passe de 15 minutes à environ 3 minutes.
- **Identification des menaces et des vulnérabilités**, avec mise en place de **mesures de prévention**.

# Les Composants de l'IAM



# Type d'identité

Les Groupes

Les  
Roles

Les  
Utilisateurs

# CONCLUSION

- IAM : cœur de la **sécurité et de l'efficacité** en entreprise.
- **Problèmes identifiés :**
  - Multiplication des identités et comptes orphelins.
  - Gestion décentralisée et coûts élevés (mots de passe, perte de productivité).

# CONCLUSION

- **Solution IAM :**
  - Gestion centralisée des utilisateurs, rôles et groupes.
  - Authentification, autorisation et surveillance.
  - Gestion des privilèges et audits.
- Objectifs atteints :**
  - Confidentialité, conformité (ex. RGPD) et sécurité.
  - Gain de temps et efficacité pour les utilisateurs.
  - Réduction des risques et prévention des vulnérabilités.

# CONCLUSION

- **Principe clé :** les bonnes personnes accèdent aux bonnes ressources ,au bon moment, pour les bonnes raisons