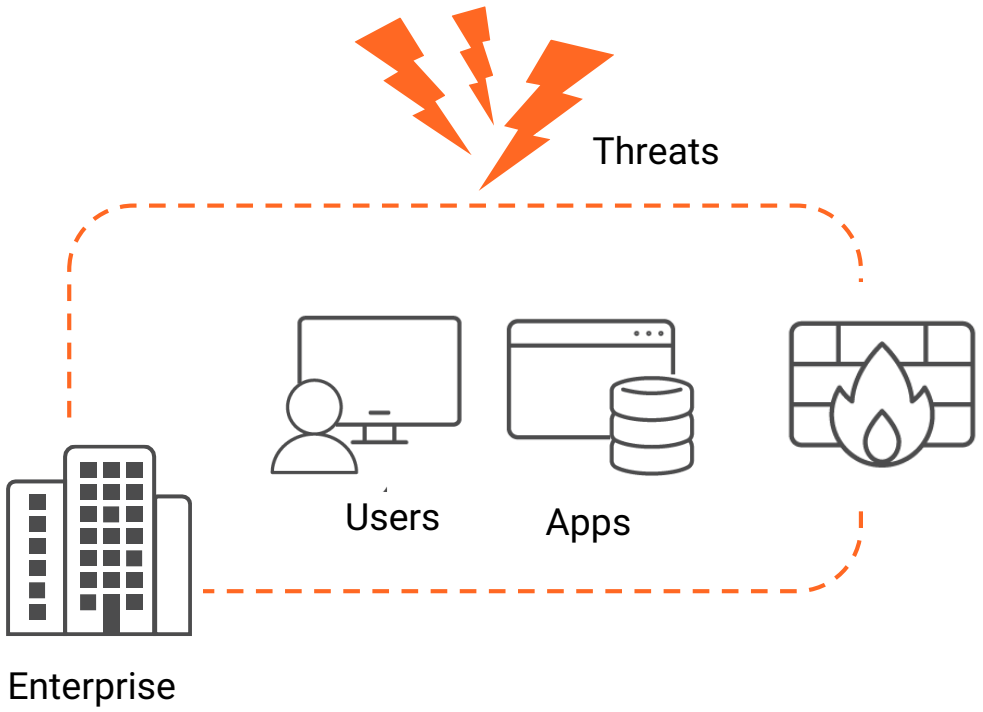
Identity and Access Management

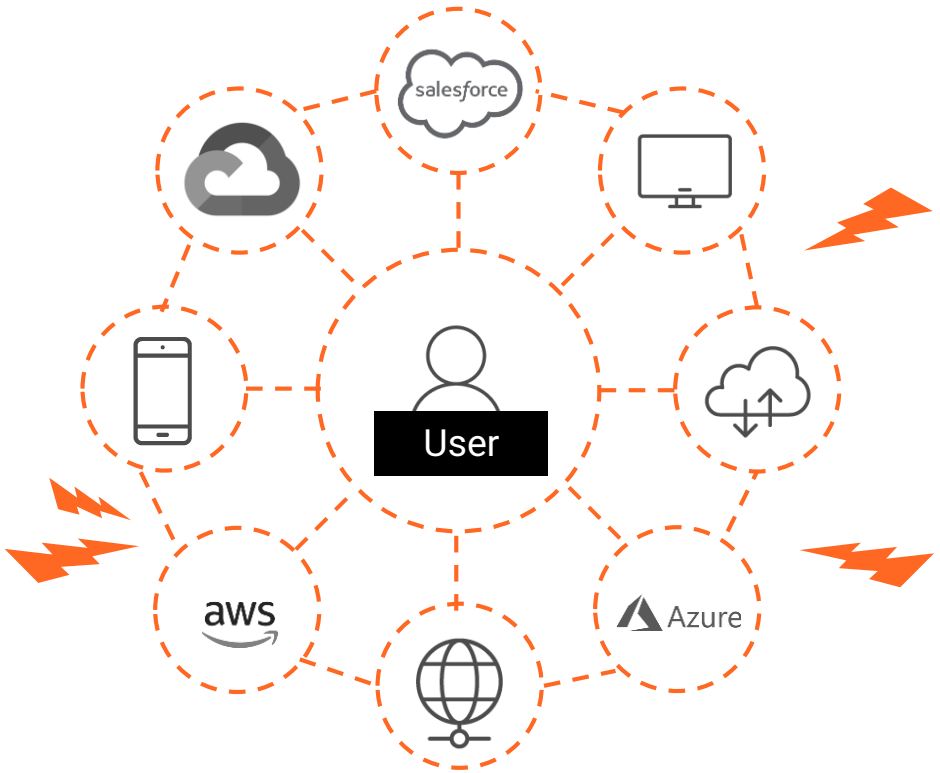
Why care about IAM in your security strategy

IDENTITY IS THE NEW PERIMETER

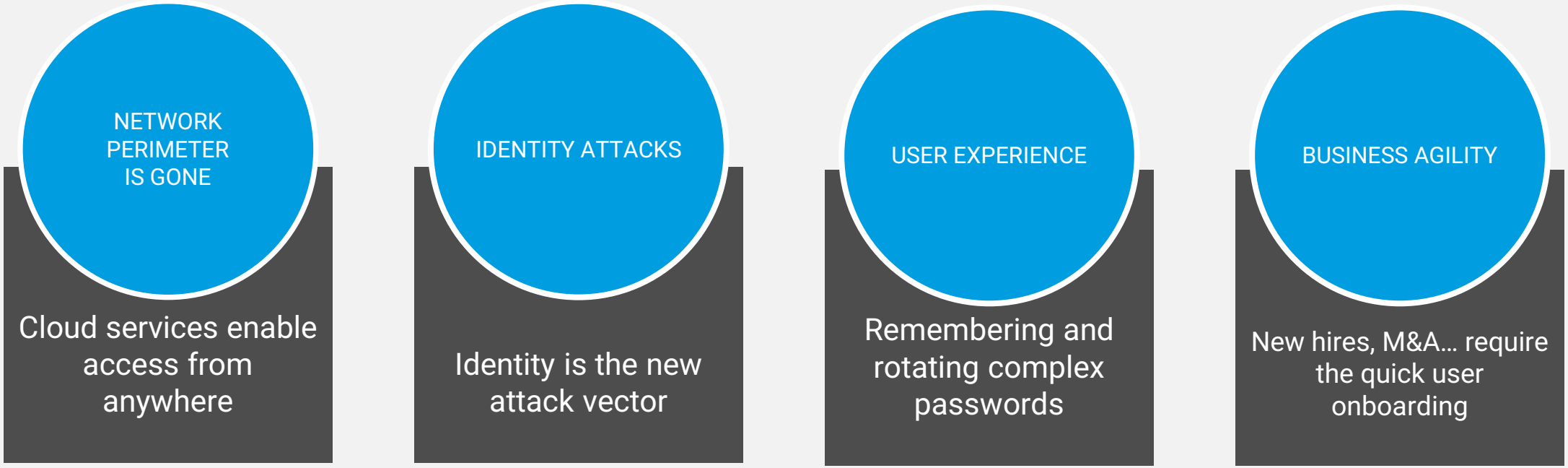
PERIMETER-BASED SECURITY
Physical & Digital Barriers



IDENTITY-DEFINED SECURITY
Continuous Verification



AUTHENTICATION CHALLENGES



SOME PASSWORD INSIGHTS

Identity is the top attack vector!

…of breaches involve weak default or stolen passwords

…of breaches involve privileged credential misuse

But users don't use a secure way to identify themselves

…of users repeat/reuse their stolen passwords

…of government and military employees' LinkedIn passwords are weak

GATES PREDICTS DEATH OF THE PASSWORD (FEB 2004)

DATA BREACHES – 10 YEAR CHALLENGE

YEAR: 2008	YEAR: 2018
1. Hacking	1. Use of stolen credentials (hacking)
2. Malcode	2. RAM scraper (malware)
3. Misuse	3. Phishing (social) (deceit)
4. Physical	4. Privilege abuse (misuse)

IDENTITY RELATED

Source: Verizon “2008 databreach investigation” & Verizon “2018 databreach investigation”

CHALLENGE 1: USER EXPERIENCE

CHALLENGES

- Slow response to service requests due to IT department intervention
- Poor user experience with multifactor authentication
- Password fatigue

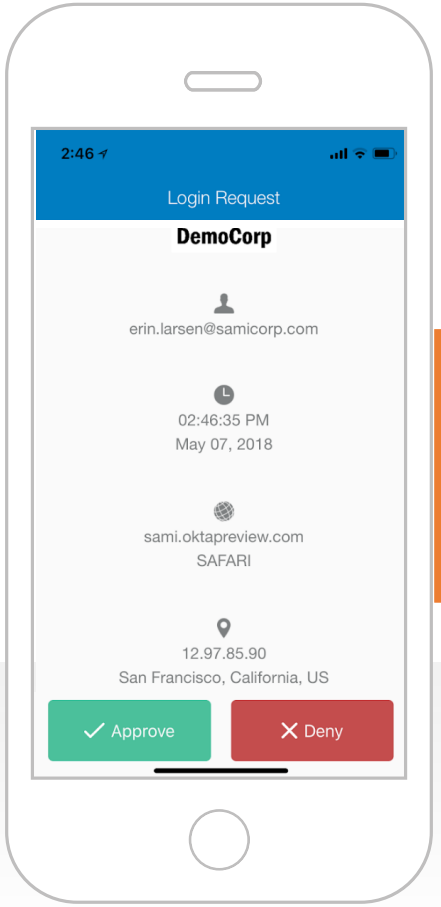
SOLUTIONS

- Self-Service
  - Self-provisioning
  - Self reset of password
  - Self management of data
- Single-SignOn
- Password-less authentication

BENEFITS

- Increased productivity
- Reduced workload on IT
- Increased employee satisfaction

SECURE PASSWORDLESS EXPERIENCE



Push Authentication

CHALLENGE 2: BUSINESS AGILITY

CHALLENGES	SOLUTIONS	BENEFITS
• Slow onboarding/offboarding to service requests due to IT department intervention	• Facilitate data flows and management processes with automation	• Increased productivity
• Lack of agility during M&A	• Centralize identity store based on rules	• Reduced workload on IT and improve speed
• Difficult enablement of partners/providers	• Make IAM an enabler with flexible self services, process support	• Increased agility and security

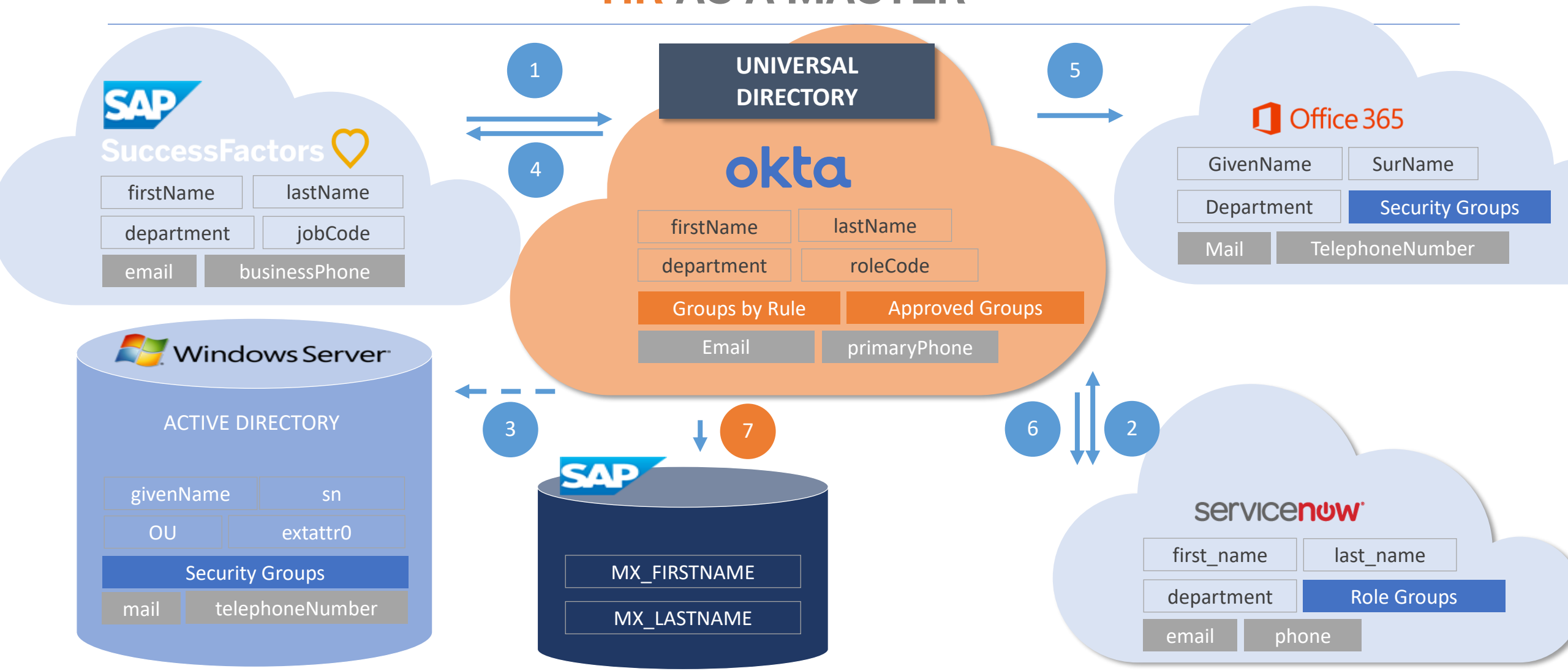
IT IS ALL ABOUT

PEOPLE

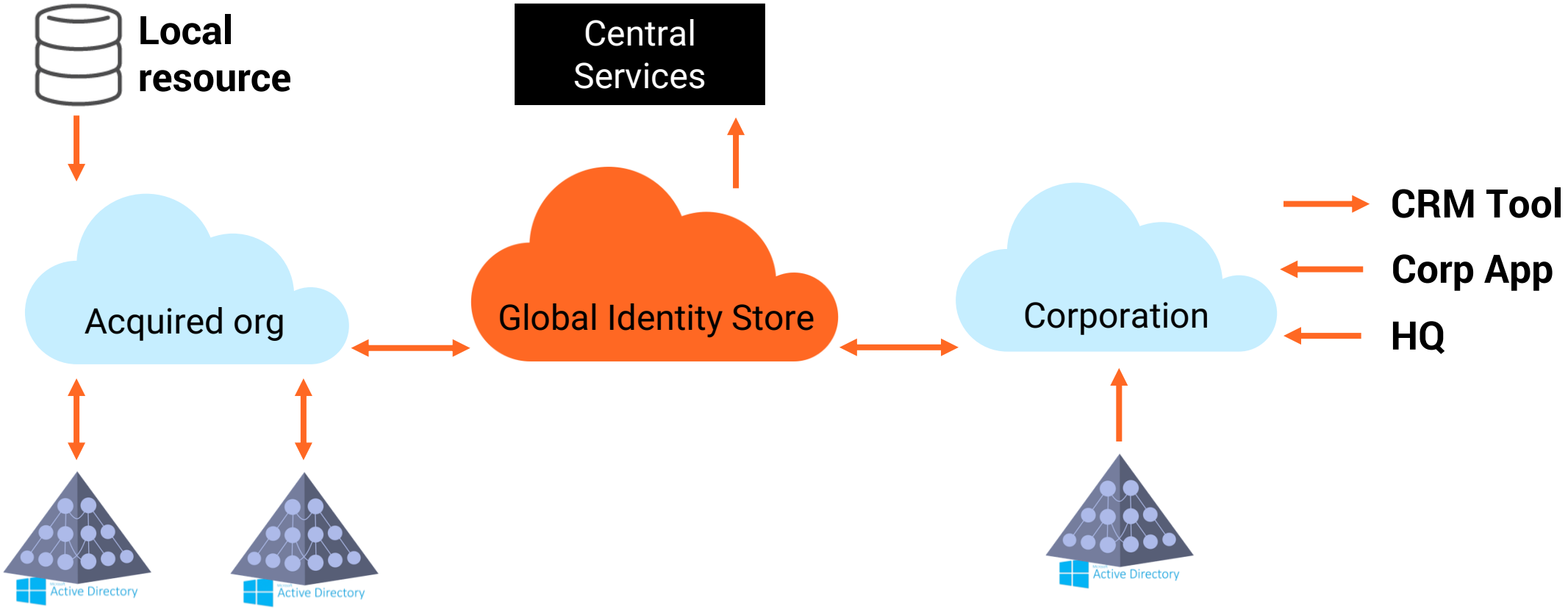
PROCESS

TECHNOLOGY

HR AS A MASTER



TARGET ARCHITECTURE for M&A

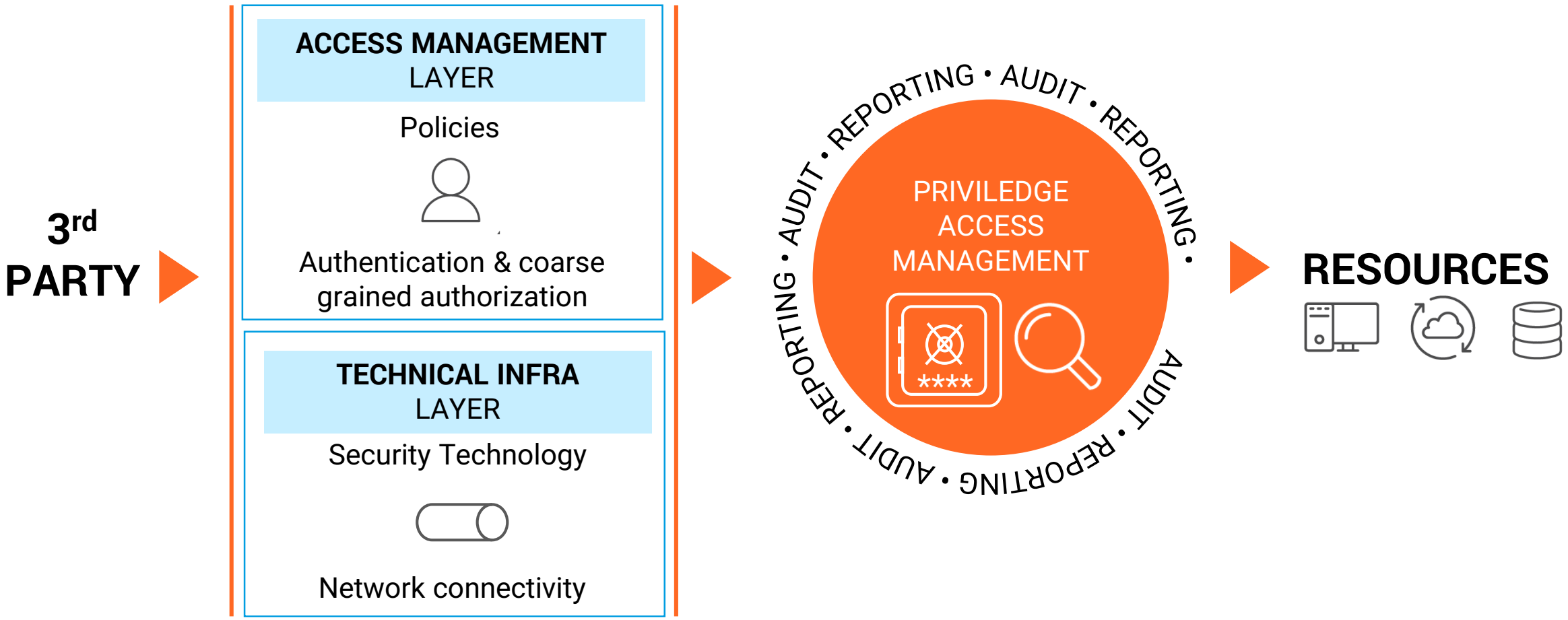


LACK OF CONFIDENCE IN THIRD-PARTY ACCESS

Some reasons why the majority of companies don’t have much confidence in third-party access:

- Lots of unknown accesses
- No clear definition of approval process
- No risk or impact analysis
- Rights are given, rarely removed
- No central user management, SSO, or sometimes pollution of internal user database
- No activity tracing

SECURING THIRD-PARTY ACCESS



SECURELINK IAM OFFERING

USER EXPERIENCE

• SaaS delivered Access Management	• Enable cloud applications with self-provisioning, self password reset, SSO & password-less authentication

PROTECT AGAINST DATA BREACHES

• Privileged Account Discovery & Audit Assessment	• Assessment service to quickly find out your current status of privileged accounts
• Multifactor Authentication	• Prevent breaches due to leaked or cracked credentials
• Privileged Access Management	• Track, secure and audit sensitive access

BUSINESS AGILITY

• Secure third-party access	• Enable secure access for third party to sensitive applications and systems
• Solving Identity Challenges after M&A	• Enable fast and secure identity integrations after M&A by implementing a global identity store


THANK YOU FOR LISTENING!