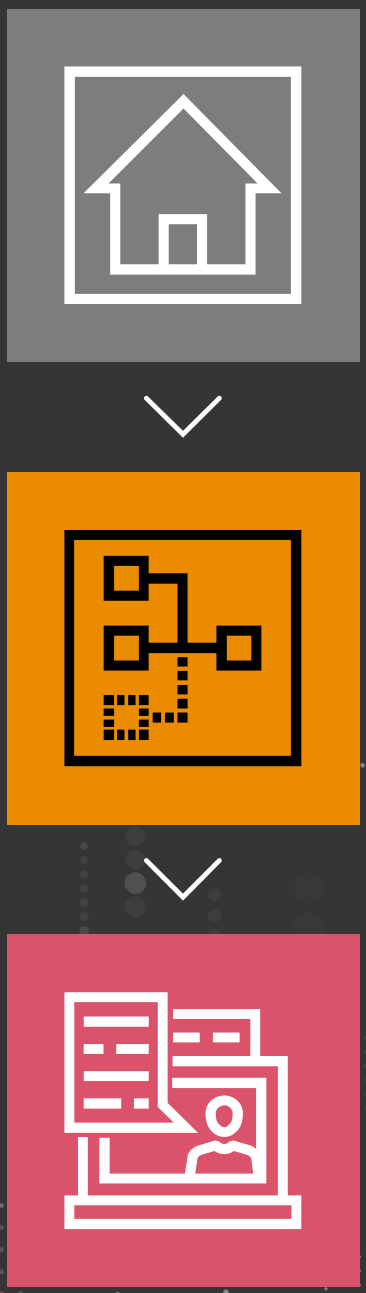
pwc

Identity and access management

Your key to seamless security

Evolution of the cybersecurity perimeters

The attack has shifted to identity.



Source: Microsoft CISO Workshop Identity and Zero Trust User Access

Trends and challenges

Identity is centric to cybersecurity in modern systems

Phishing allow attackers to impersonate valid user identities.

Modern applications are primarily identity focused in provisioning of access rights.

Passwords aren’t enough to protect identities

Single factor authentication (Passwords) without context isn’t enough assurance.

Attacks on credentials circumvent software assurances (Without hardware isolation).

Identities being used outside network

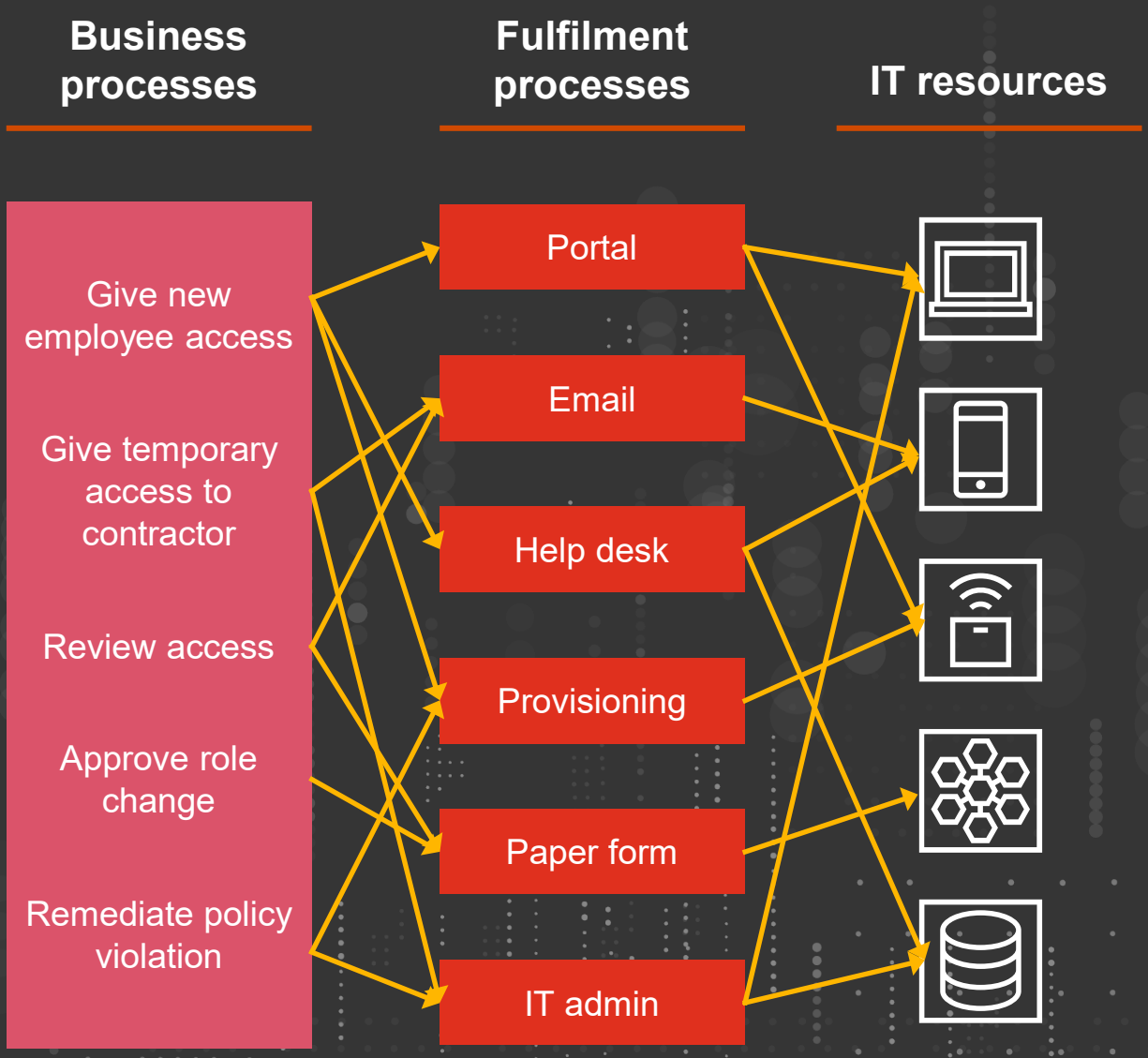
Cloud, mobile, and IoT assets are frequently beyond reach of enterprise firewalls.

Identity and access controls are inconsistent on different cloud services and devices.

Source: Microsoft CISO Workshop Identity and Zero Trust User Access

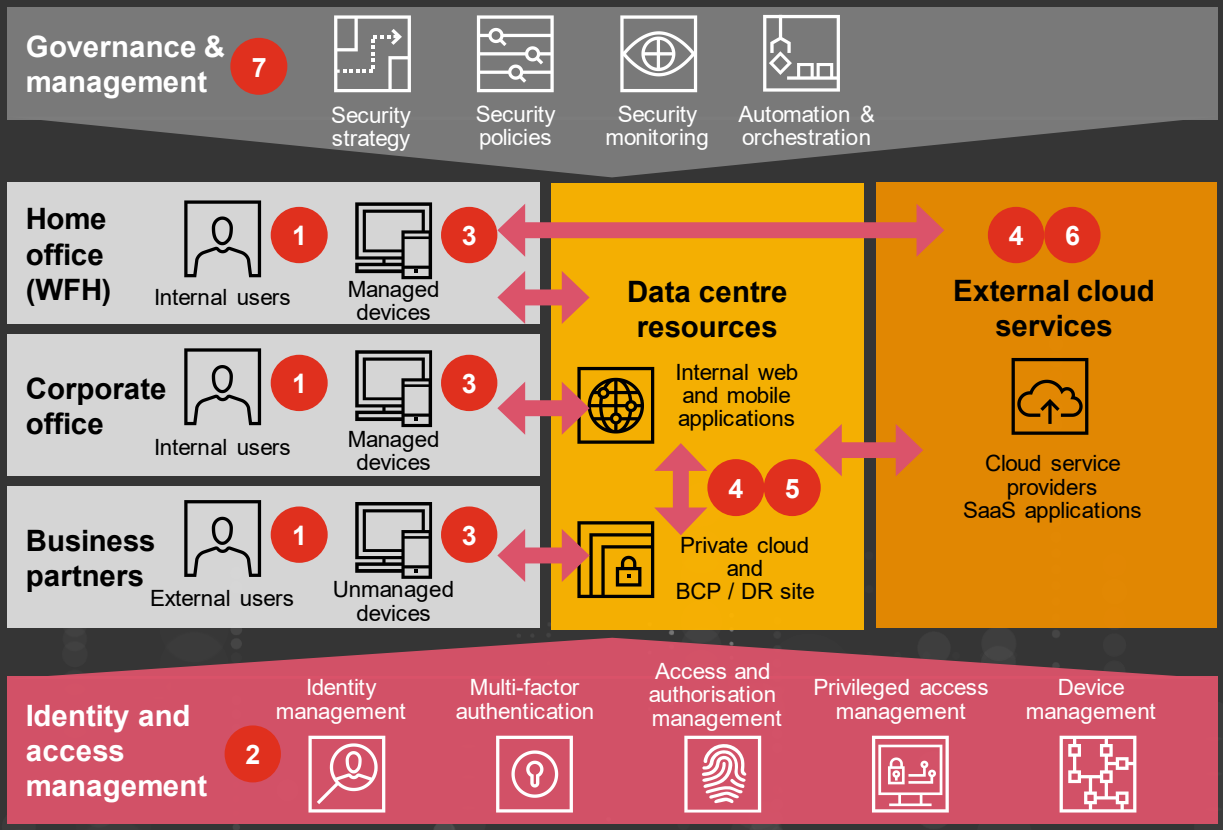
Client pain – “The harsh reality of identity today”

- Organisations continue to struggle with managing user access
- Identity business processes are inefficient and service levels are unpredictable
- Business user experience is inconsistent and disjoined
- Implementation of consistent, reliable controls is impossible



Identity is at the heart of a Zero Trust design strategy

This is an example of a tailored Zero Trust Framework PwC developed for a client. These are aligned with global industrial standards such as National Institute of Standards and Technology (NIST) Special Publication 800-207 and Zero Trust Maturity Model that was issued by the Cybersecurity and Infrastructure Security Agency (CISA) in April 2023.



1. **Identity – Software defined access**
   Users and devices are authenticated before gaining access to the internal network. Rules are applied dynamically based on identity and access context.
2. **Identity – Identity and access management**
   Identity is at the heart of a Zero Trust strategy only to allow entitled internal and external users access to appropriate resources with proper authorisation.
3. **Devices – Secure endpoints**
   Endpoint security controls are applied to users and devices (including mobile) before remotely accessing data centre or cloud resources.
4. **Networks – Micro-segmentation**
   Applications & servers are segmented by projects with limited communication with each other. Unauthorised traffic is blocked to/from data centres, the private cloud environment, and business continuity and/or disaster recovery sites.
5. **Workloads and data – Software-defined perimeter**
   Policy-driven and context-aware segmentation for securing remote access and site-to-site communications.
6. **Workloads and data – Secure cloud networking**
   Leverage scalable secure cloud services to govern user access to resources from anywhere.
7. **Visibility and analytics and automation and orchestration governance and management**
   Strategy, policy management, and continuous real-time monitoring are critical to programme success.

Key focus areas for identity and access management

Based on our experience, identity and access management (IAM) should be approached holistically to include all disciplines listed below.

Enterprise IAM is focused on identity governance and administration, access management, and privileged access management.

Security and experience uplift

Access management (AM)

Enable the adoption of modern standards and protocols for authentication, MFA, and controlling access.

- Portal
- Application integration patterns
- Multi-factor authentication (MFA)
- Authentication and authorisation

Consumer identity and access management (CIAM)

Improve and simplify user experiences throughout their life cycle, from user sign up to sign in and self-service.

- Identity proofing
- Self-service password management
- Progressive profiling
- Preference management

Security focused

Privileged access management (PAM)

Mature the use cases to better monitor and govern privileged accounts and password.

- Privileged account discovery and onboarding
- Password rotation
- Service and system account management
- Session governance and logging

Foundational

Identity governance and administration (IGA)

Establish a resilient programme that automates provisioning, review, and life cycle of users through modern technologies and processes.

- HR source of truth integration
- User onboarding and offboarding
- Access request and approvals
- Access reviews

Successful case sharing

PwC was engaged in an IAM project for a large luxury fashion company. The project involved review on in-house applications' access account, role assignment and permissions as well as standard operating procedures and guidelines.

Current state

The client has a large number of applications involving user accounts for staff and external vendors within APAC.

- 40+ pioneer applications without review on access and role assignment
- Inconsistent role design for each application
- Inadequate documentation and guidelines on IAM
- Different applications are being managed and supported by external vendors who owned excessive permission right in an application
- Instructions given but not effectively executed by application owners
- SSO or MFA are not enforced

Why was this happened?

- A lack of collaboration and communication between different teams and departments responsible for role design and application functionality. Plus no coordination or sharing of best practices, each application developed its own role design independently
- Application owners do not have a regular practice to monitor on outsourcing management. As internal teams may have less control over how applications are managed and maintained by vendors who may not have the same level of security protocols and standards as internal teams
- No comprehensive review and alignment of roles and access across applications
- Failure to consistently integrate SSO or apply MFA for accessing to the application and no regular review on logon activity

How did PwC help?

- PwC helped client to conduct the core pioneer applications' access and role review
- Designed roadmap per reviewed applications for ongoing improvement on IAM controls and execution
- Revisited the SSO and MFA coverage across all company related applications
- Recommended a well defined and systematic approach with the aid of identity governance and administration solution to manage and enforce access and role certifications and request application
- Proposed usage of privileged access management solution to upskill and cater the operation needs on privileged accounts as well by establishing a formal authentication and authorisation workflow

Contact us

South

Kenneth Wong
PwC Mainland China and Hong Kong
Cybersecurity and Privacy Leader
kenneth.ks.wong@hk.pwc.com

Kok Tin Gan
Partner, Cybersecurity and Privacy
kok.t.gan@hk.pwc.com

Jenius Shieh
Partner, Cybersecurity and Privacy
jenius.h.shieh@hk.pwc.com

Yen Hoe Lee
Director, Cybersecurity and Privacy
yen.hoe.lee@cn.pwc.com

Kevin Lam
Senior Manager, Cybersecurity and Privacy
kevin.lam@hk.pwc.com

Central

Chun Yin Cheung
Partner, Cybersecurity and Privacy
chun.yin.cheung@cn.pwc.com

North

Lisa Li
PwC Mainland China
Cybersecurity and Privacy Leader
lisa.ra.li@cn.pwc.com