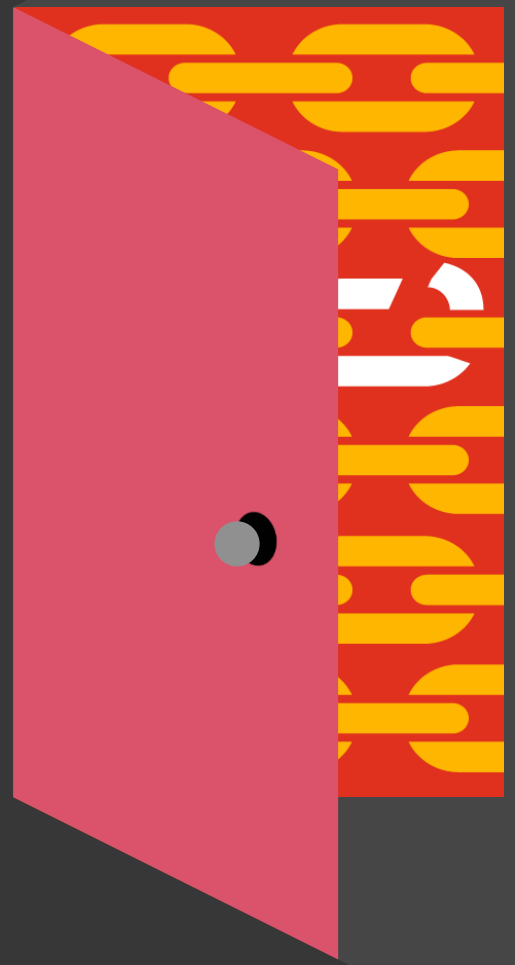
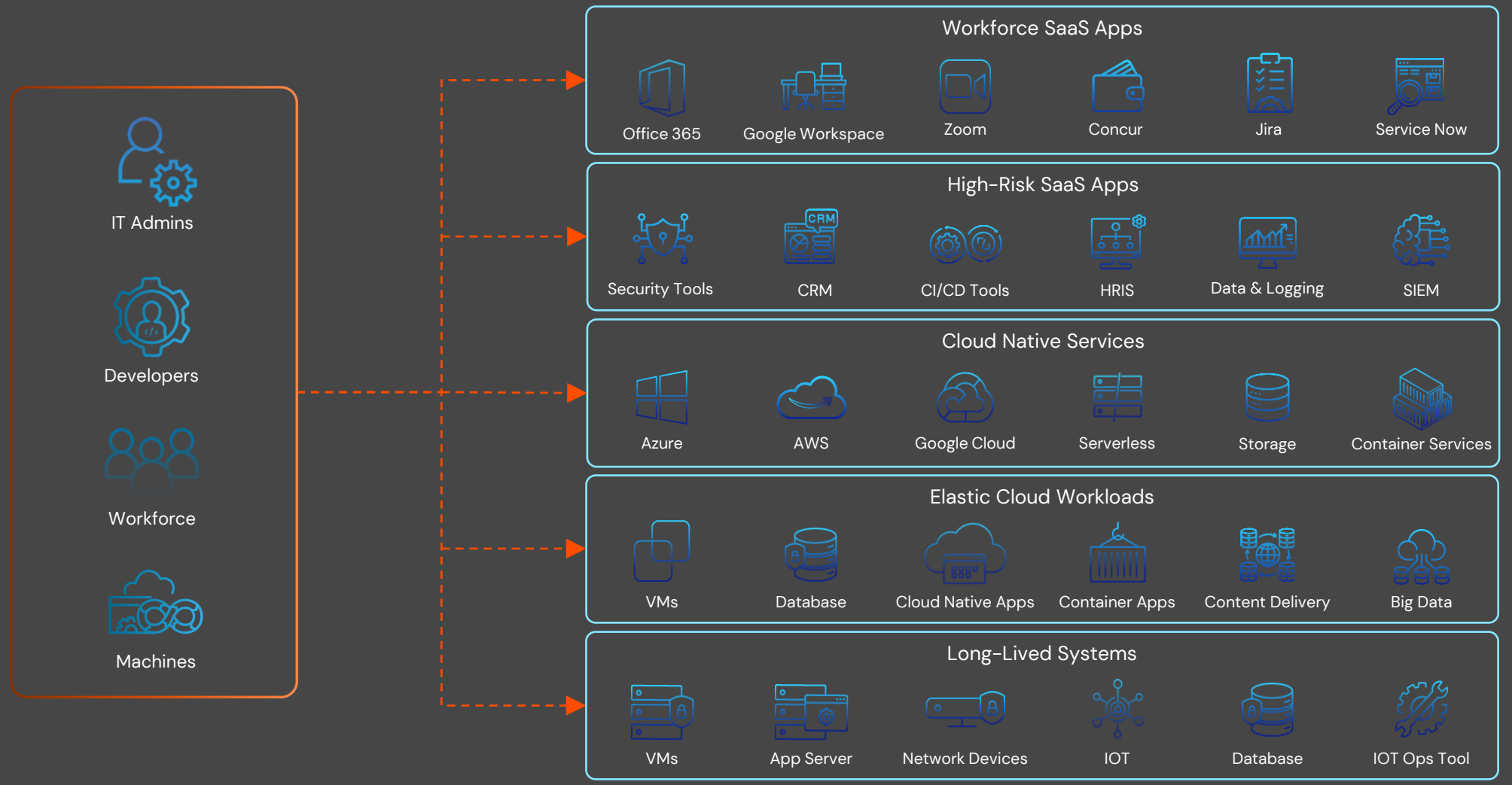
Modern PAM

Præsentation af Martin Topgaard, Senior Manager, PwC Danmark



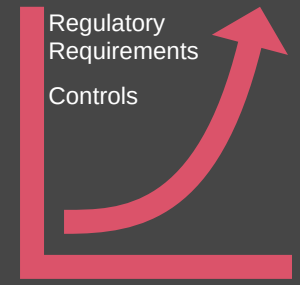
The Classic PAM solution can’t keep up….

- **New ways of working requires JIT access to dynamic ressources**
- **New types of systems and accesses**
- **New types of secrets like short lived certificates and Tokens**
- **Business users are becomming privileged in business applications**



More – More – More ....

More Vendors



More Regulations

Explosion of Cloud Entitlements

Along with the explosion of cloud services and entitlements, has come a corresponding explosion of privileged accounts across all environments.

Amazon Web Services (AWS) features and services:

- 2006: 3 services (S3, SQS, EC2)
- 2013: 25
- 2018: 95
- 2019:149
- 2020: 283
- 2021: 300+

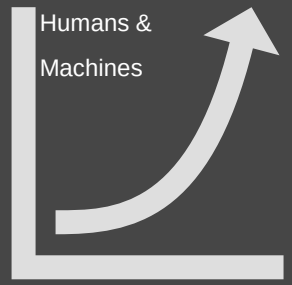
Explosion of multicloud permissions

- 7,100+ AWS Identity and Access Management (IAM) permissions (approximately 2,500 in 2017)
- 5,000+ Microsoft Azure IAM permissions
- 3,200+ Google Cloud Identity and Access Management (IAM) permissions

Gartner

More Secrets

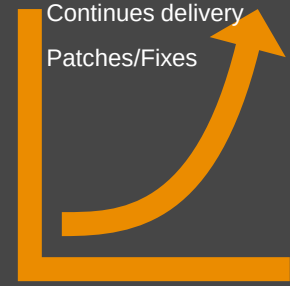
More components



More Identities

More Requests

More Security Threats



More Changes

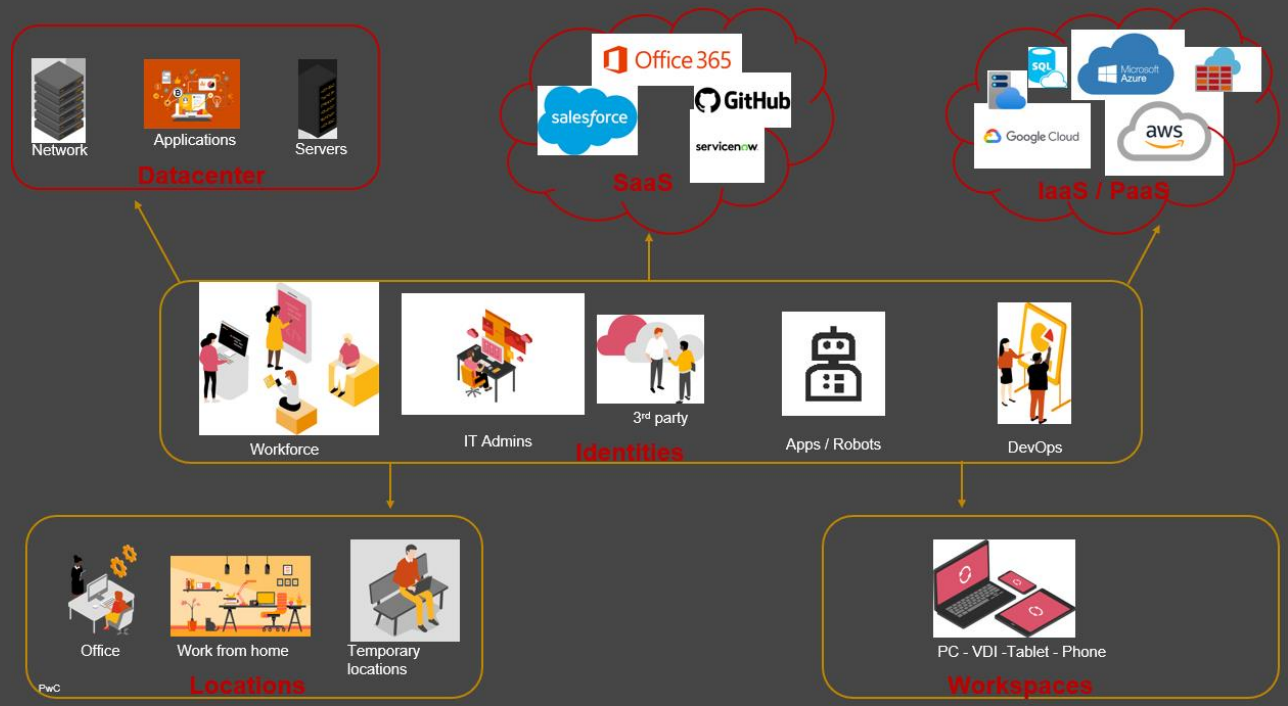
IAM & PAM challenges in the hybrid cloud

Privilege sprawl caused by lack of clear roles and responsibilities

Cloud vendors implementation of identity and access management are inconsistent

Existing controls are challenging to use in all hybrid/multi cloud environment

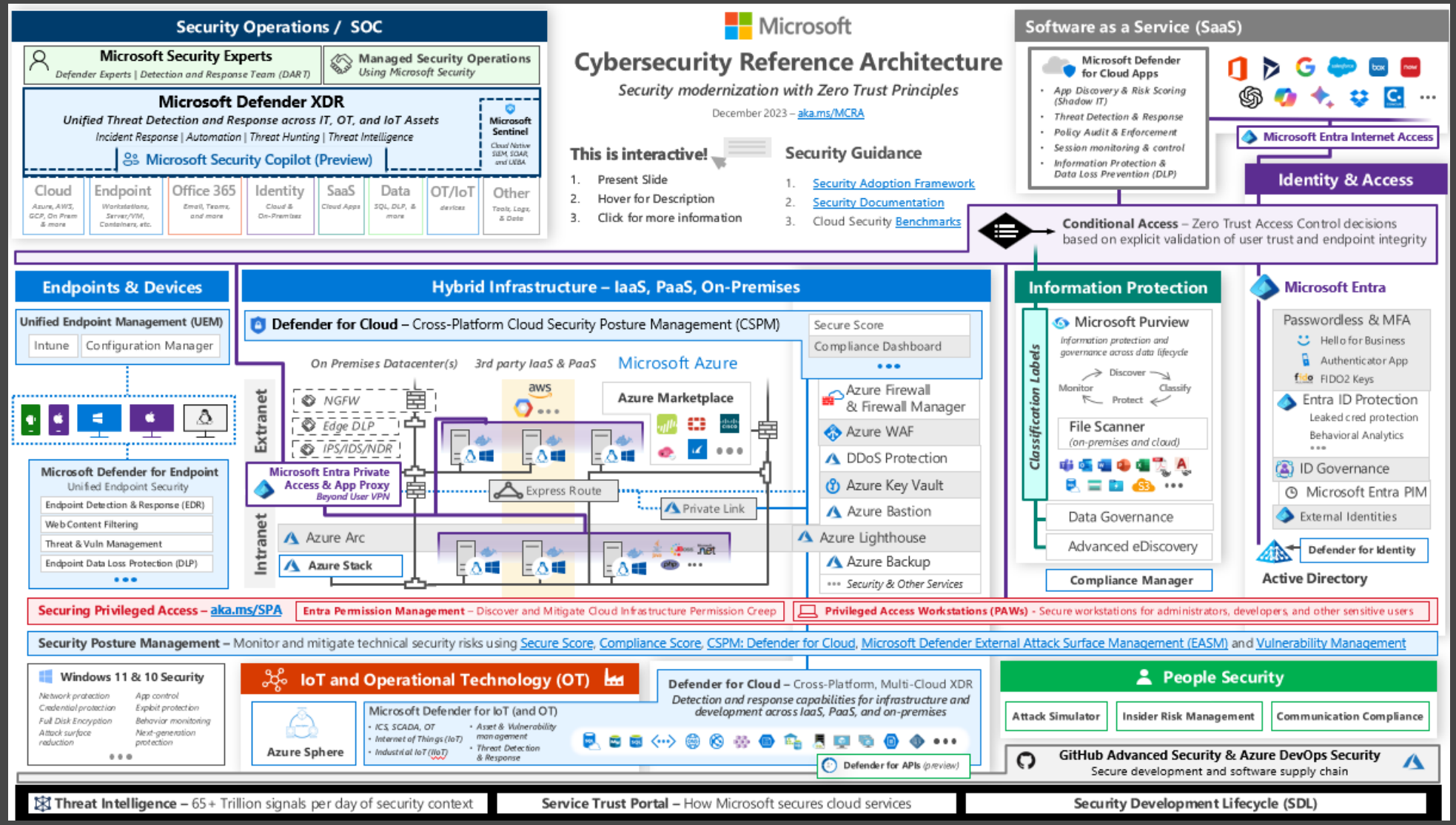
Existing IAM & PAM tools are not a good fit for agile workloads in the cloud



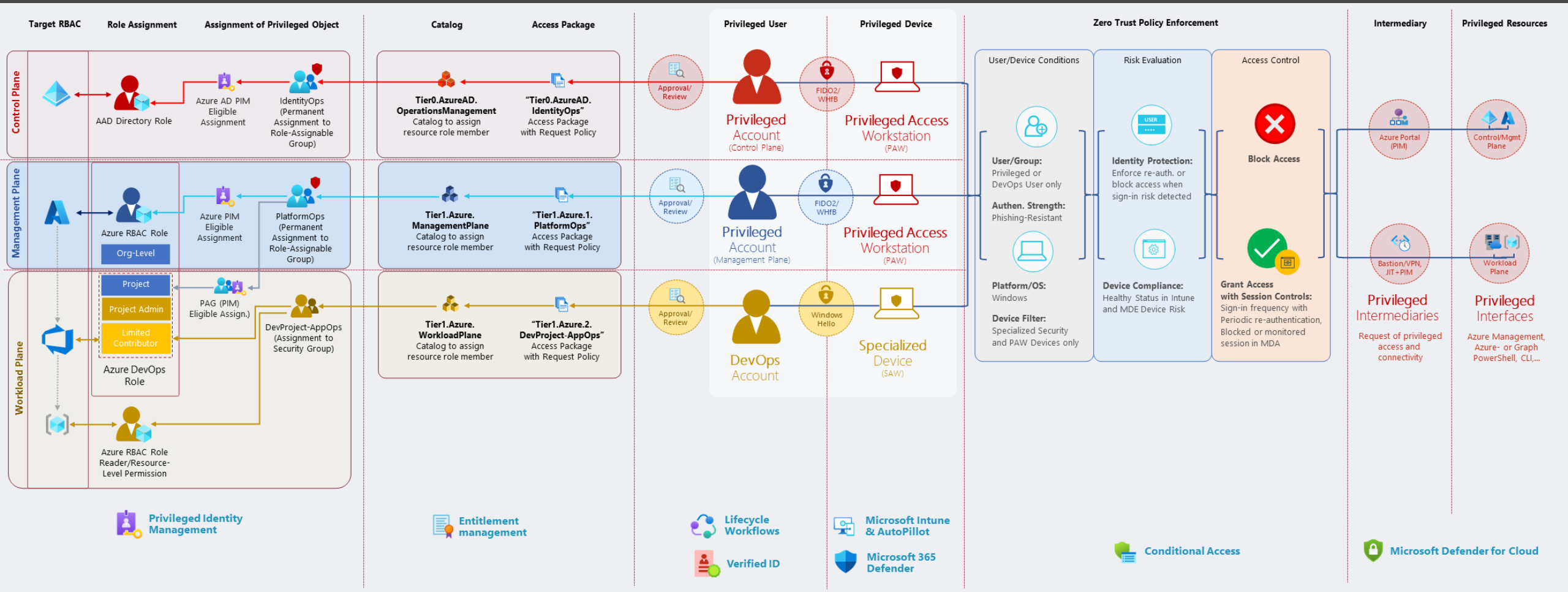
Cloud vendors native IAM & PAM controls requires multiple platforms and licenses

3´rd party vendors and consultants manages & operate cloud services/applications

The ”New” Governance Challenge



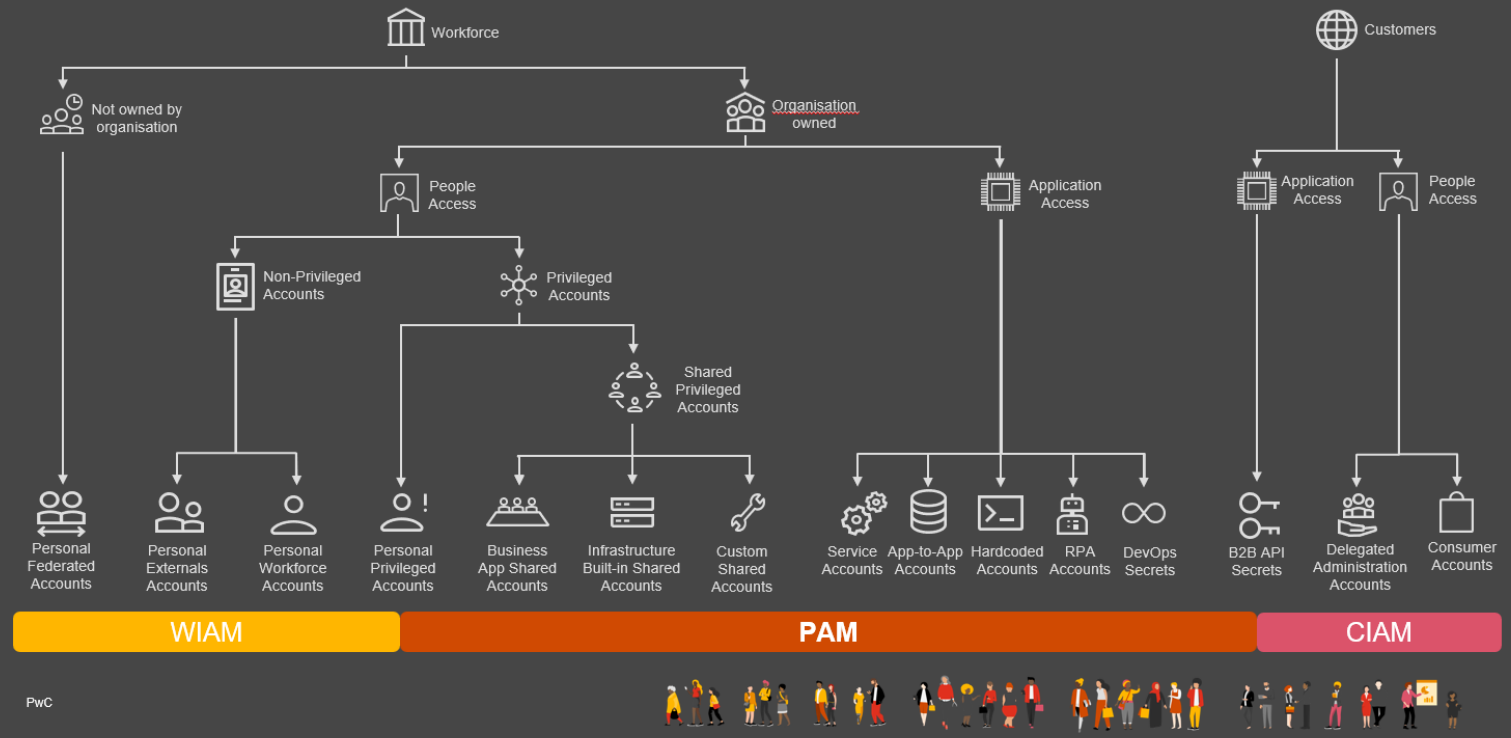
Microsoft Azure PAM model



Are you in control of your Identities in the hybrid cloud?

- **Do You know and understand your current risk associated with all types of Identities?**
- **Do you have the right controls implemented for all identities according to the risk?**

- Do you re-evaluate risks when consuming new services from existing platforms or new types of threats are detected?
- Do you continuously detect over privileged accesses and revoke them?
- Do you have the right controls implemented for all identities according to the risk?



Protect Identities across organization

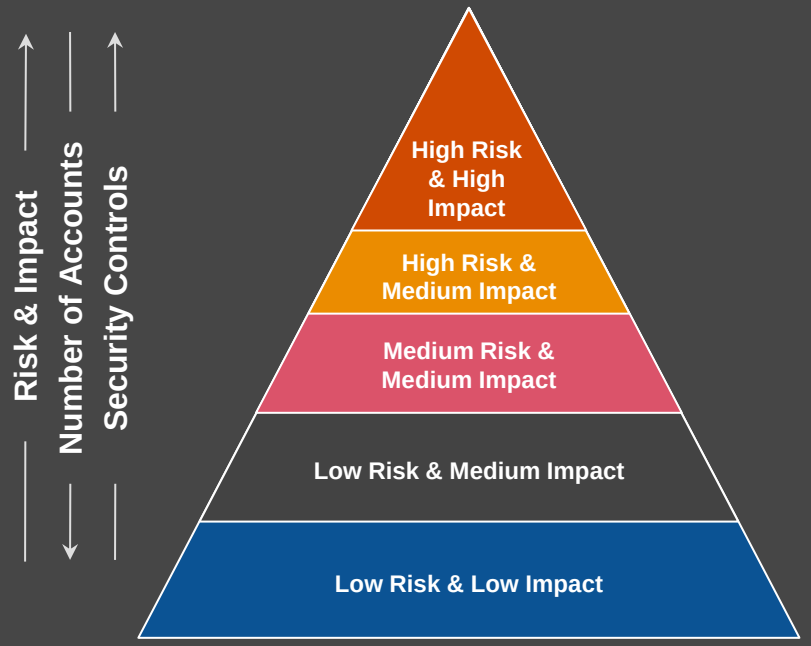
Almost every attack starts by taking over identity of an account within the breached organization.

Having automated streamlined IAM processes is a key to protect your assets and to allow efficient work for your employees and to be compliant with all regulatory and audit requirements

Before enforcing controls

Below are some key considerations to be made before enforcing controls:

- Develop an inventory of services and impact & risk of compromise
- Assess types of access according to business impact & risk
- Define privileged access types
- Discovery of privileged access
- Identification of tiers based on tiering matrix
- Hygiene Exercise on accounts
- Updating the controls model to meet the standards
- Finalizing the tools for enforcing controls
- Setting up necessary integrations to allow enforcement



Controlling the hybrid cloud

Define privilege access

- Access to manipulate critical business data?
  - HR data, source code, customer data….
- Access to admin cloud portals/API's
- Access to workloads & DevOps tools
- …

Apply a consistent, effective security policy across all hybrid cloud resources

- Strong identity verification with MFA
- Device verification
- Least privilege access
- Just in time access
- User friendly experience

Define privilege access controls

- Assess the criticality of the access
  - What is the risk if the access is compromised
- Can JIT be assigned based on user attributes?
- Is session isolation/monitoring required?
- Is Credential rotation required?
- Is additional MFA policies required?
- How should workload credentials be controlled

….

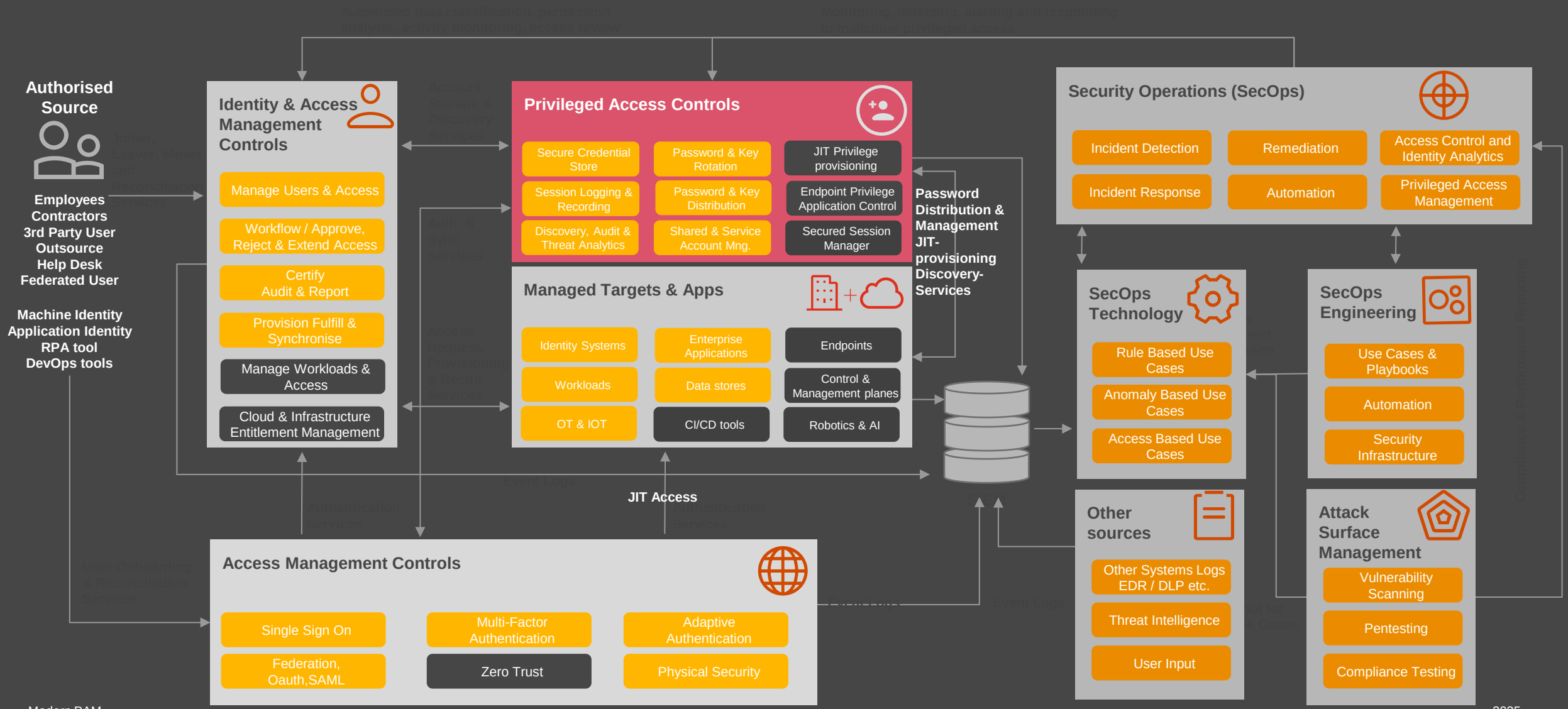
Automate processes

- Use scanning tools to detect unused credentials and entitlements
- Use attribute based access control to ensure scalability and agility
- Use IAM system to manage identities

Training

- security awareness training
- cross training security operations

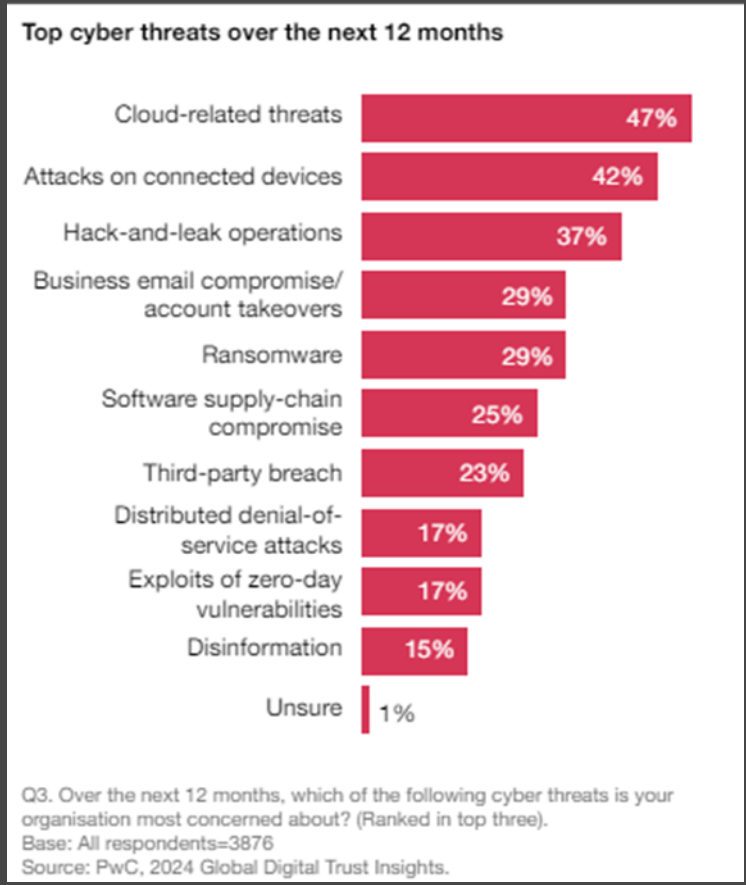
Integrated Identity Security for hybrid cloud



Is the foundation in place?

When shifting from an on-premises system to a cloud-based system, you should reevaluate your existing policies and procedures to determine whether your existing expectations apply to the cloud environment, and which adjustments may be needed to accomodate the shared-responsibilities model.

- **Do you have a common controls framework?**
  - Has it been tailored to address technology in the cloud? If not,
    - what barriers have prevented you from tailoring your controls and whose involvement is needed to resolve those barriers?
- **Have you assigned systems ownership for your cloud-based assets?**
  - As part of that ownership, have you provided adequate training in evaluating cloud risks and the relevant controls executed by either the CSP or your own management to support an effective control environment?
- **How are you monitoring for adherence to your common control framework and onboarding new technologies/assets?**
  - Who is responsible?
  - On what cadence is this monitoring performed?
  - How have you updated your feedback loop to incorporate the results of monitoring into your risk assessment and related controls mapping?



Thank You

www.pwc.dk

Together we succeed…