Identity and Access Management

Built for Microsoft Azure
Active Directory

pwc | Microsoft

Identity and Access Management (IAM) overview

Identity is at the core of how we help our clients

Achieve authorised access at any time, from anywhere, by employees, business partners, and customers.

Cloud security

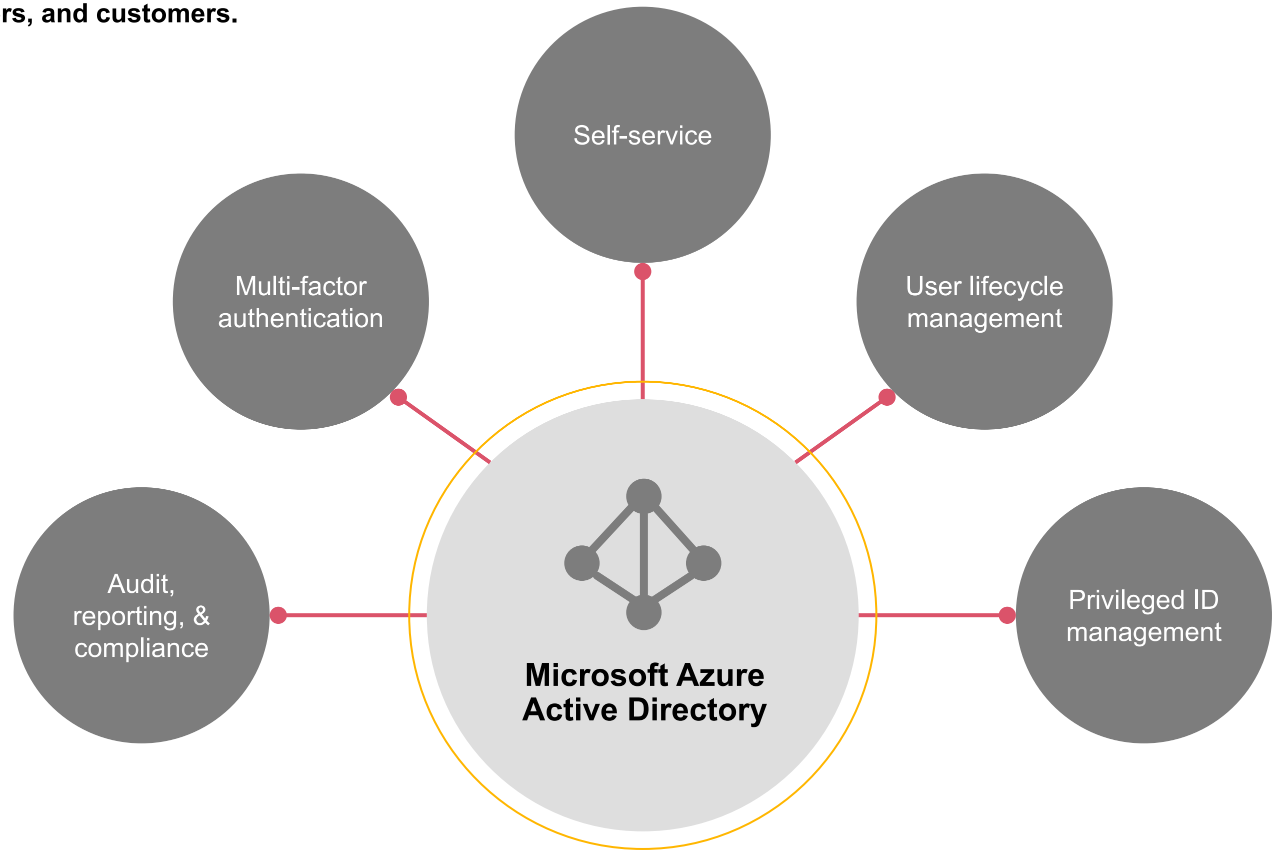
Extend identity and access management to cloud-based applications

Controlled access

Use the latest context-aware authentication process to increase security

Self service

Resolve your own issues with self service, reducing IT cost to services and improving user experience


Self-service
Multi-factor authentication
User lifecycle management
Audit, reporting, & compliance
Microsoft Azure Active Directory
Privileged ID management

1

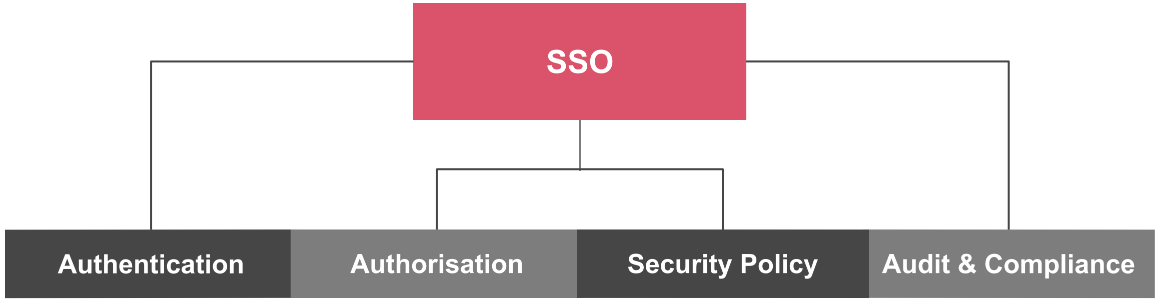
Single Sign-On (SSO)

Single Sign-On (SSO) overview

SSO provides a consistent, centralised approach for authentication and session management across an organisation's applications and resources.

Key questions addressed

- Do users in your organisation use multiple user IDs and Passwords to access the different applications within the enterprise?
- Is your Help Desk fielding an unreasonable number of Password Reset calls? Do users write passwords down because they can't remember them all?
- Do you understand and control who has access to which web-based applications?



Key benefits

Increased user productivity: Enable faster and easier access to applications and information throughout the business process lifecycle of an organisation. Only one account generation request (one ID one password) is required.

Reduced Help-desk Costs: Decrease the number and expense of help desk password resets by reducing the number of id/password combinations to be managed by the end user

Decreased Downtime: Users are not spending time waiting for the Help Desk to reset a password and/or understand which ID is required to access which application

Enhanced Application Security: Establish a central security infrastructure to control access to all applications. Common authentication and authorisation policies can be enforced across the application base.

Enhanced Password Security: A centralised repository allows for more effective password policies and controls.

Secure and Seamless Integrations: A centralised access management system provides a secure and easy integration for applications, to provide user authentication and single sign-on capabilities.

Reduced Audit/Compliance Overhead: A Centralised system facilitates an one stop shop for audit reporting of application security controls (e.g., who has access to what?)

Enhancing user experience & application security – Single Sign-On (SSO)

As organisations increasingly adopt cloud-first strategies, consistent authentication experiences plus extending the authentication security beyond the perimeter requires adoption of a standards compliant access management platform that will enable enhanced authentication both internally and externally. Furthermore, different stakeholders within an organisation face different sets of challenges for implementing enhanced authentication security:

CIO

- Enterprise Change Management
- Reduction of on-prem technology footprint
- Large variance in authentication experience
- Cost reduction by leveraging existing solutions
- Adherence to industry standards and regulations

CISO

- Rapid scalability & availability
- Removing the need for multiple passwords across applications
- Standards based solution for enhanced security and easy integration
- Maintenance & support overhead from managing partner identities

IAM Team

- Maintenance overhead due to disparate non-standard authentication solutions
- Ability to rapidly deploy and integrate with different types of applications
- Self service password management and application on boarding
- Reduce infrastructure footprint

Deployment & Integration Complexity

- Dealing with RADIUS and non-federated applications
- Coordination with application and infrastructure teams
- Seamless migration from existing solution.

Reporting

- Focus on addressing suspicious login attempts
- Fine grained logging of authentication attempts to monitor load and to facilitate rapid troubleshooting.
- Focus to automate monitoring and response capabilities

Azure AD as your IAM solution

Azure AD is Microsoft’s Cloud IAM (IDaaS solution) that provides Single Sign-On capability to both on premise and SaaS applications. You can leverage most of Azure AD’s SSO features with your O365 license!

SSO

Single Sign-On capability for up to 10 applications at a time, with your O365 license, for both on-premise and SaaS cloud hosted applications. SSO for unlimited applications with Premium license.

MFA

Enable Multi Factor Authentication for all your Azure AD integrated applications at no extra cost, included with your O365 License.

AD Connect

Azure AD Connect allows synchronisation of on-prem AD identities with Azure AD & provides multiple options to enable SSO in a hybrid environment. Azure AD connect license is included with your O365 license.

B2B Integration

Capability to extend SSO to your applications for up to 5 external users per license is included with your O365 license. This allows for seamless onboarding of clients onto your applications, significantly reducing operational overheads.

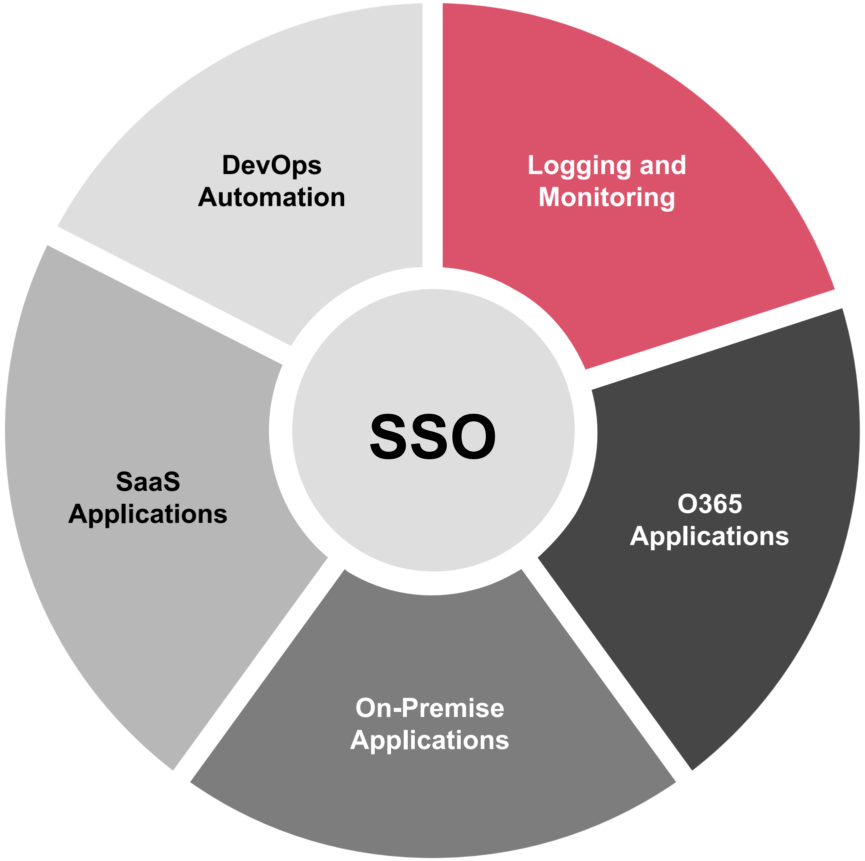
Conditional Access

With an Azure AD premium license you can enable conditional access which allows for policy based MFA enforcement. This provides flexibility to enforce MFA based on context, user role, group membership etc.

Identity Protection

Azure AD identity protection enables automatic detection and remediation of identity based risks. It provides the information required for real time adaptive authentication decisions based on various risk factors. A premium license is required.

Building a centralised access management solution



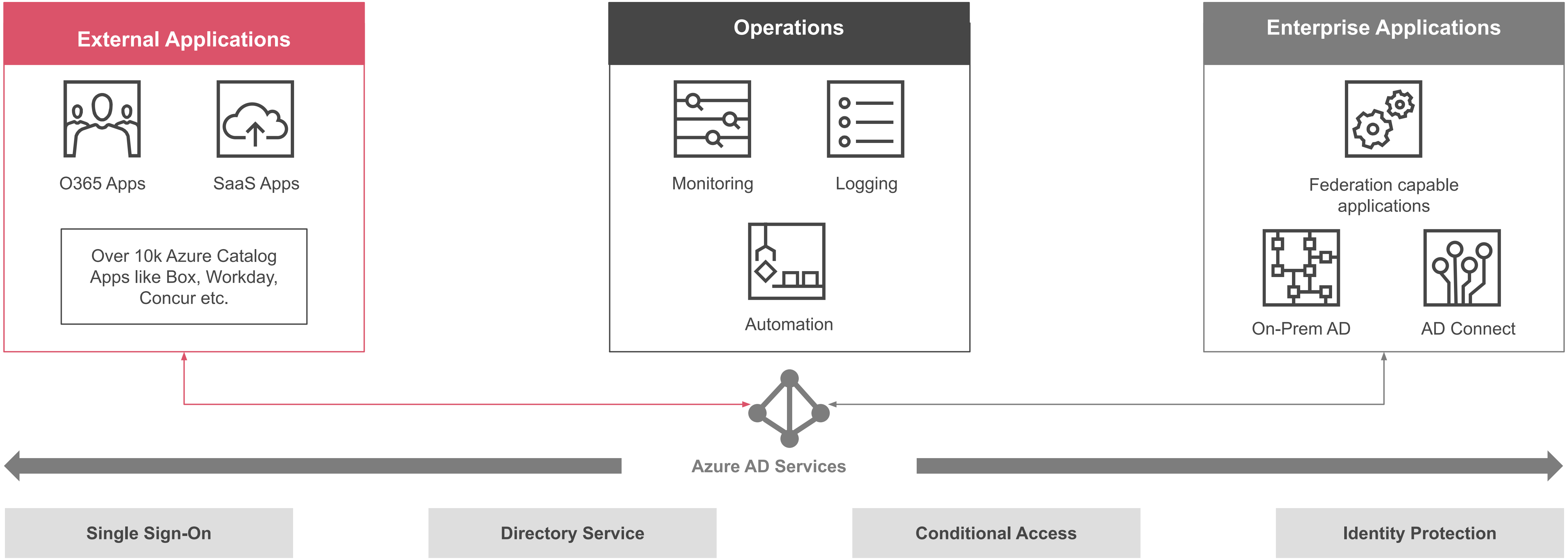
Microsoft technologies

- Enable integration with a wide range of applications, supporting different authentication protocols (SAML, RADIUS, etc.).
- Support for key SSO capabilities including with standard O365 subscription.
- Support seamless onboarding of on-prem AD users on to O365.
- Advanced adaptive access policies for enhanced security.
- Integration with SIEM solutions for efficient logging and troubleshooting.

PwC professional services

- Build and configure your Single Sign-On platform to cater for the client's standard and complex use cases.
- Implement solution for coexistence with existing SSO solution.
- Integrate the solution with the client's SIEM and incident management tools.
- Establish processes and automation using devops toolkits via a hybrid on-site and remote team.
- Integrate pilot set of applications for different use cases and document integration standards for rapid onboarding of applications.

Azure AD architecture overview



External Applications

O365 Apps

SaaS Apps

Over 10k Azure Catalog Apps like Box, Workday, Concur etc.

Operations

Monitoring

Logging

Automation

Enterprise Applications

Federation capable applications

On-Prem AD

AD Connect

Azure AD Services

Single Sign-On

Directory Service

Conditional Access

Identity Protection

PwC accelerators – Rapid onboarding model

PwC’s streamlined onboarding framework will enable you to overcome the challenges presented by environment size and disparate authentication systems. It will increase the velocity and effectiveness of onboarding applications and end users while reducing related costs.

Increasing onboarding velocity — Our onboarding accelerators will speed up processes to onboard to Azure AD platform. The bottom line: You’ll realize value from your IAM technology and services investments more rapidly.

The path to achieve rapid onboarding

Tailor the rapid onboarding model to your needs
Enhance your onboarding model that allows you to increase the velocity and effectiveness of onboarding applications and end users while reducing the costs to do so

Build an IAM application self-service portal for seamless migration
Develop a self service portal to stage application metadata (e.g., endpoints, certificates) and user/application guides for faster onboarding

Perform capacity planning and scalability based on deployment schedules
Assess large migrations that will involve heavy loads and traffic to the access management platform to avoid outages

Standardise integration patterns
Having a defined, repeatable, proven process combined with data driven services and features will lead to automation

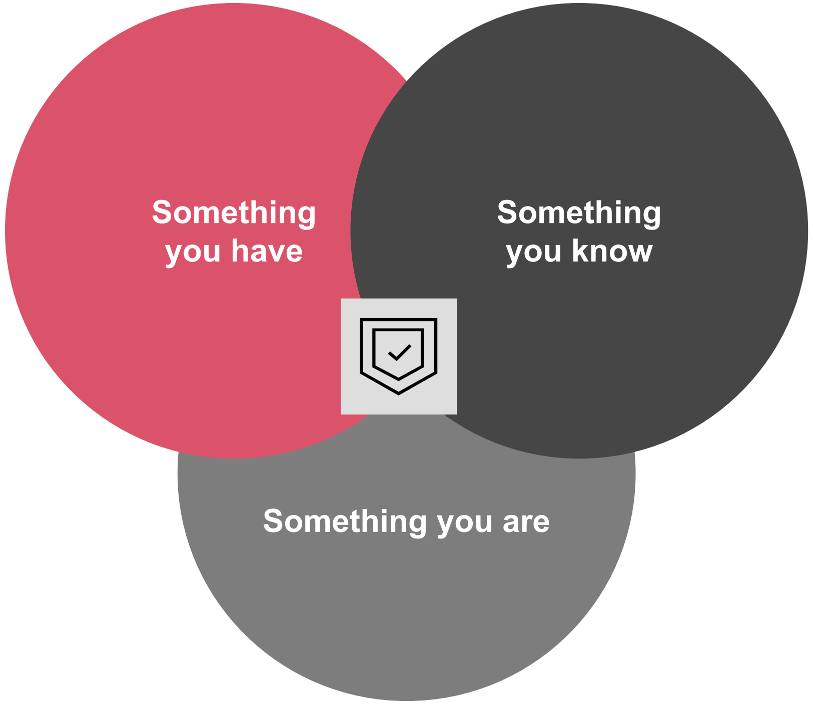
Benefit	Impact
Greater efficiency and speed to on-board an asset	• Quicker ROI for the IAM Solution • Increased velocity of onboarding volume
Use of standard IAM Service processes and tools, implementation of leading practices	• Lower risk • Improved quality
Use of optimised methods and tools for standard implementation paths	• Specialised processing • Reduce time to complete
Defined, repeatable, proven process and results	• Cost effective, high quality, improved predictability, reduce time to complete
Reduced process handoffs between various participants	• Lower task complexity • Reduce risk of dropping balls
Continuous optimisation of processes	• Process improvement
Pool of dedicated specialists	• Optimised staffing, availability, flexibility
Leverage specialised knowledge and skills	• Optimised task execution

2

Multi-factor Authentication

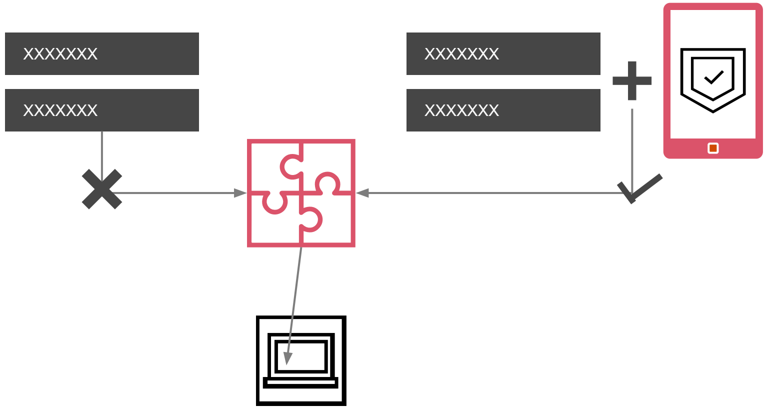
Why Multi-Factor Authentication (MFA)?

Multi-Factor Authentication extends authentication security beyond username and password (something you know) to include something you have and/or something you are. This creates a unique authentication experience which increases the ability to validate and trust the authenticated user.



- Leverage multiple factors (credential set, delivered one-time token, or biometrics) to increase authentication security
- Ability to enable end-user compliance with industry best practice and regulations
- Expand identity validation to be consumed by other self-service functions such as password reset
- Expand integrations usage through Integrated Windows Authentication & Single Sign On

MFA can be utilized to protect against phishing and password spray attacks by adding an additional authentication requirement, often it is a function available currently to Office365 clients.
A basic username and password authentication can be exploited via stolen credentials or brute force attack



What are your concerns?

As organisations increasingly adopt cloud-first strategies, consistent authentication experiences plus extending the authentication security beyond the perimeter requires adoption of a multi-factor authentication toolkit that will enable enhanced authentication both internally and externally. Furthermore, different stakeholders within an organisation face different sets of challenges and concerns when implementing enhanced authentication security:

CIO

- Enterprise Change Management
- End User Token Fatigue
- Large variance in authentication experience
- Flexibility of number of MFA factors
- Cost Reduction on Self-Service Resets

CISO

- Rapid scalability & availability
- Protection from password related attack vectors
- Adherence to industry standards and guidelines on MFA factors

IAM Team

- Consistent enrollment process
- Role based ability to reset factors for end-users to enable Help Desk operations
- Ability to rapidly deploy and test expansion of MFA

Deployment & Integration Complexity

- Dealing with RADIUS and non-federated applications
- Coordination with application and infrastructure teams
- Seamless migration from existing solution.

Reporting

- Focus on addressing suspicious login attempts
- Fine grained logging of authentication attempts to monitor load and to facilitate rapid troubleshooting.
- Focus to automate monitoring and response capabilities

Enterprise MFA capabilities

PwC’s streamlined onboarding framework will enable you to overcome the challenges presented by environment size and disparate authentication systems. It will increase the velocity and effectiveness of onboarding applications and end users while reducing related costs.

Increasing onboarding velocity — Our onboarding accelerators will speed up processes to onboard to Azure AD platform. The bottom line: You’ll realise value from your IAM technology and services investments more rapidly.

Addressing enterprise risk

Enhance Business Security
Enabling multi-factor authentication can be used to enhance the security not only for internal user communities and resources, but can be utilised to help provide external users with additional account protection

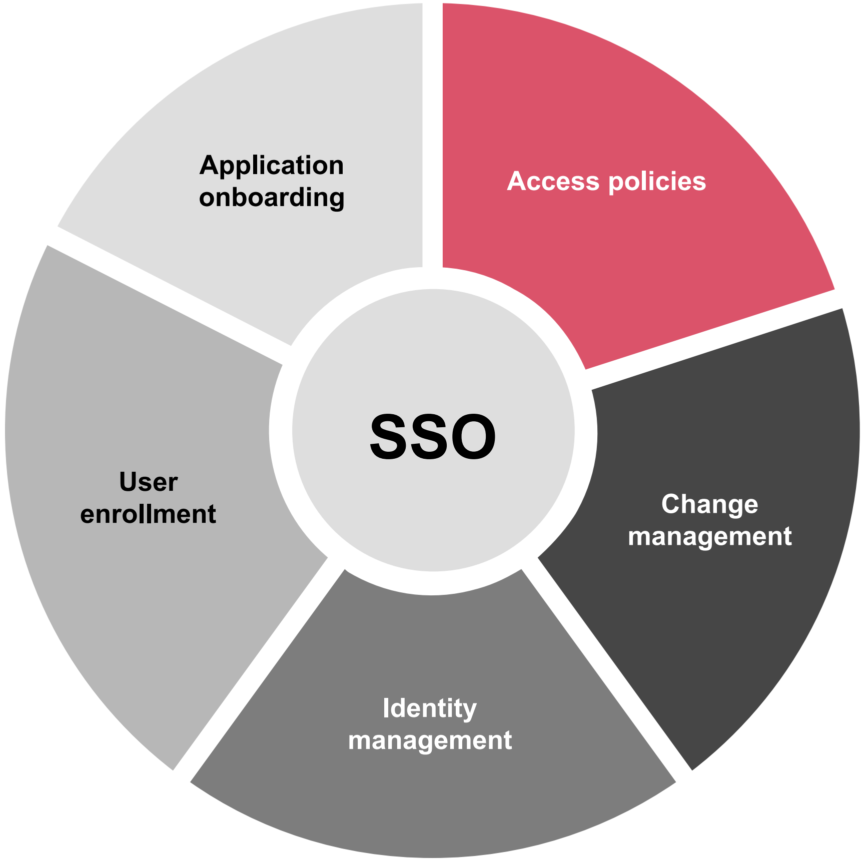
Address Risk and Compliance
Protecting the enterprise by reducing risk and addressing compliance related restrictions for authentication to sensitive applications

Identity as the new Perimeter
The cloud enabled landscape requires security considerations to be placed on the identity with multi-factor authentication utilised as the primary driver for validation

Integrate Operational Processes
Multi-factor authentication helps increase security for privileged accounts by utilising additional authentication requirements when accessing production applications

MFA capabilities	Description
Token Factor Availability	Should provide end-users a variety of token factors for completing MFA prompt
Risk Based Claims	Should provide additional considerations for risk based logins such as country or IP designated constraints
Mobile Capability	Should give users the ability to utilise a mobile accessible factor
One-time Passcode	Should allow for one-time passcodes in the event a user is unable to complete the verification prompt
Device Restrictions	Should allow for restricting claims based on device trust
Seamless Integration	Should be capable of integrating with a variety of applications, infrastructure appliances, or access management solutions

Building an integrated MFA solution



Microsoft technologies

- Integrate with your existing IAM capabilities (i.e. identity management, application provisioning, etc.)
- Enhance perimeter applications and cloud-native integrations to close immediate security gaps
- Facilitate future growth and scaling in line with your business needs
- Utilise current Enterprise Licensing to deploy enhanced security functionality

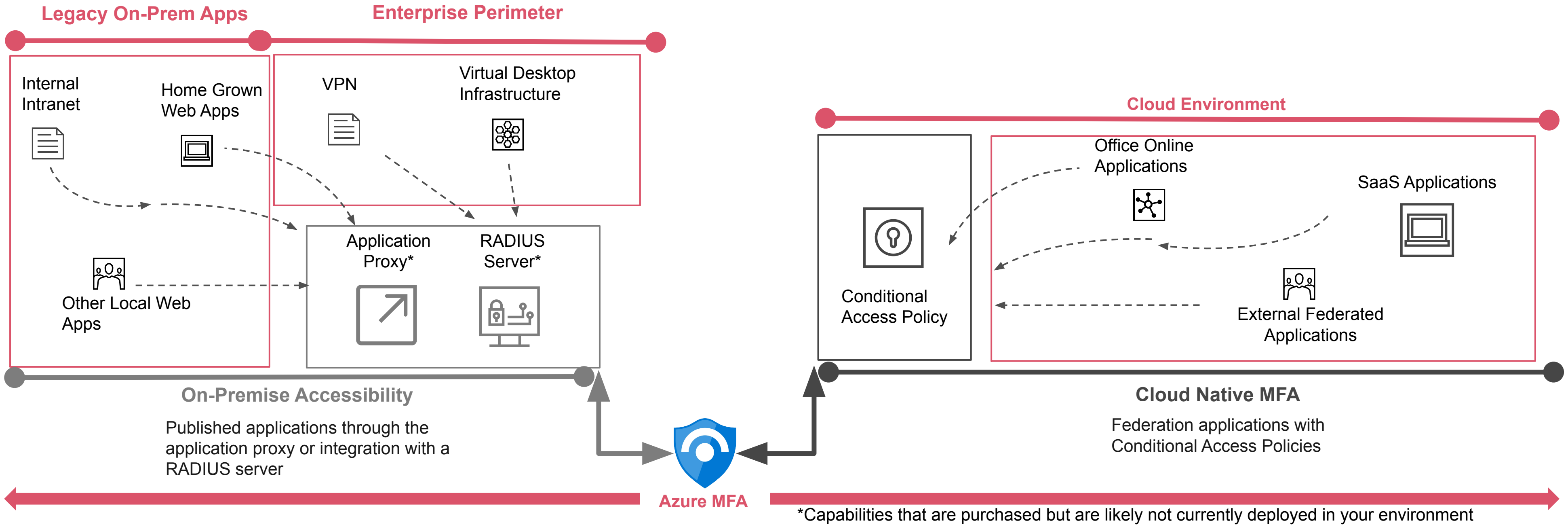
PwC professional services

- Address complex but manageable use cases by deploying Azure MFA on your behalf
- Develop reporting functionality (e.g., unenrollment reports, failed authentication attempts, etc)
- Established change management process and creation of artifacts for enterprise onboarding
- Enable industry leading security practices rapidly to adapt to remote access use across enterprises

Integrated architecture overview

PwC will partner with your IT organisation to help design and implementation a holistic solution to address the primary needs of the organisation. Our experience gives us the unique capability to address security concerns, enterprise architecture needs, and end-user adoption with an integrated approach utilizing your organisation's current technology investments.

Integrate All Applications with Azure MFA



Published applications through the application proxy or integration with a RADIUS server

Federation applications with Conditional Access Policies

*Capabilities that are purchased but are likely not currently deployed in your environment

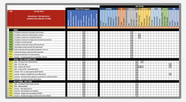
Microsoft & PwC capabilities

PwC has extensive implementation and operational experience with Microsoft products. Our experienced personnel help accelerate MFA deployments by utilising architecture blueprints, leading engineering practices, and change management accelerators collected from a variety of engagement experiences.

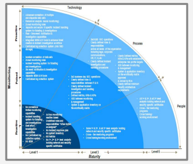
Our teams have experience with various leading MFA products, along with a security driven approach that helps our clients identify how to utilise these toolsets to their full extent.

Key accelerators

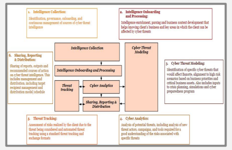
MFA Integration and Design



Prioritised integration roadmap based upon current risk rating



Token Factor Use Case Development



1. Intelligence Collection: Identification, governance, onboarding, and continuous management of sources of cyber threat intelligence

2. Intelligence Onboarding and Processing: Intelligence enrichment, parsing and business content development that helps knowing client's business and key areas in which the client can be affected by cyber threats

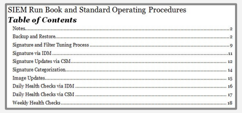
3. Cyber Threat Modeling: Identification of specific cyber threats that would affect Banorte, alignment to high risk scenarios based on business priorities and critical business assets. Also includes inputs to crisis planning, simulations and cyber preparedness program

4. Cyber Analytics: Analysis of potential threats, including analysis of new threat actors, campaigns, and tools required for a good understanding of the risks associated with specific threats

5. Threat Tracking: Assessment of risks realized by the client due to the threat being considered and automated threat tracking using a standard threat tracking and exchange formats

6. Sharing, Reporting & Distribution: Sharing of reports, outputs and recommended courses of action on cyber threat intelligence. This includes management and distribution, including target recipient management and distribution model/schedule

Authentication Reporting

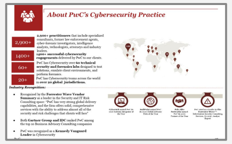


SIEM Run Book and Standard Operating Procedures

Table of Contents

Notes........2
Backup and Restore........2
Signature and Filter Tuning Process........9
Signature via IDM........11
Signature Updates via CSM........12
Signature Categorization........14
Image Updates........15
Daily Health Checks via IDM........16
Daily Health Checks via CSM........17
Weekly Health Checks........18

Change Management Planning and Artifacts



About PwC's Cybersecurity Practice

2,900+ — **2,900+ practitioners** that include specialized consultants, former law enforcement agents, cyber-forensic investigators, intelligence analysts, technologists, attorneys and industry leaders.

1400+ — **1400+ successful cybersecurity engagements** delivered by PwC to our clients.

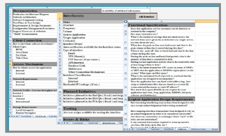
60+ — PwC has Cybersecurity over **60 technical security and forensics labs** designed to test solutions, emulate client environments, and perform forensics.

20+ — PwC has Cybersecurity teams across the world in **over 20 global jurisdictions.**

Industry Recognition:

- Recognized by the **Forrester Wave Vendor Summary** as a leader in the Security and IT Risk Consulting space: "PwC has very strong global delivery capabilities, and the firm offers solid, comprehensive services with the ability to address almost all of the security and risk challenges that clients will face"
- Both **Gartner Group and IDC** ranked PwC among the top 10 Business Advisory Consulting companies
- PwC was recognized as a **Kennedy Vanguard Leader** in Cybersecurity

Help Desk Runbooks



3

Windows Hello For Business

Passwords, why are they still around?

Personal & sensitive information is at risk for individuals & enterprises alike - password compromises result in monetary and reputation damages.

Enterprises traditionally created best of breed security capabilities; Consumer IAM solutions however have outpaced them in the last decade innovating widely adopted and more secure authentication methods that do not use traditional passwords (e.g. touch ID, face ID, Authenticator Apps), leaving Enterprise users lagging.

In 2017, 80% of breaches occurred due to poor password management processes.

The Path forward

Industry shift towards password-less

By 2022 - 60% to 90% of mid and large sized organisations will implement passwordless technologies in more than 50% of their use cases.

Intelligent solutions to improve the Security Posture

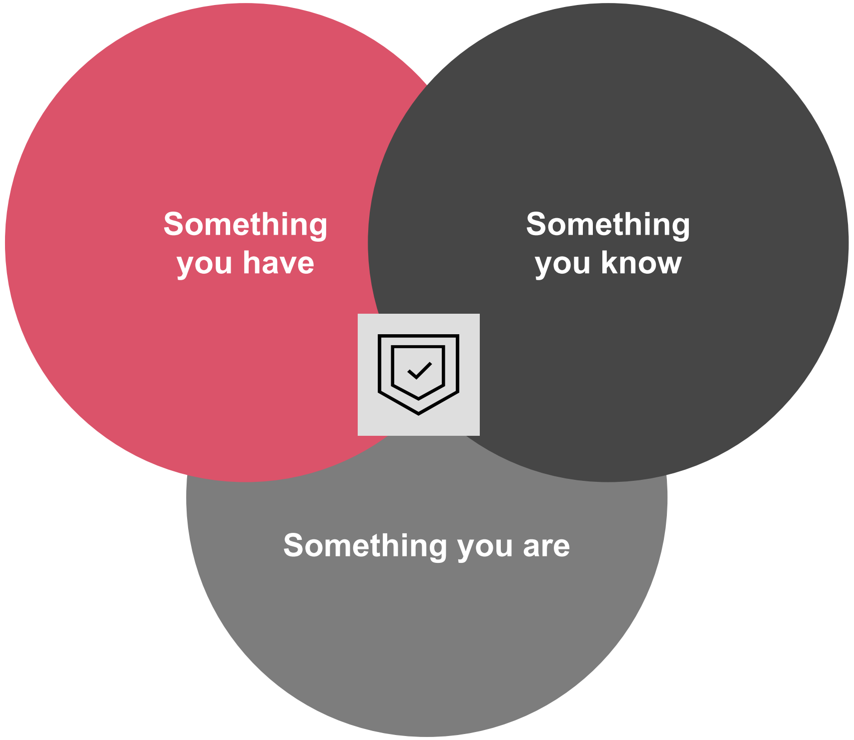
Use of strong authentication factors, biometrics, FIDO2 and other mechanisms in lieu of passwords, increases protection of personal and enterprise assets.

Increasing Efficiencies

Password reset calls received by Enterprise IT services on average cost $25 per call. The cost to migrate a workforce away from Passwords is rapidly dropping.

Unleash frictionless login

Secure and streamline access to everyday systems while avoiding ‘critical friction’

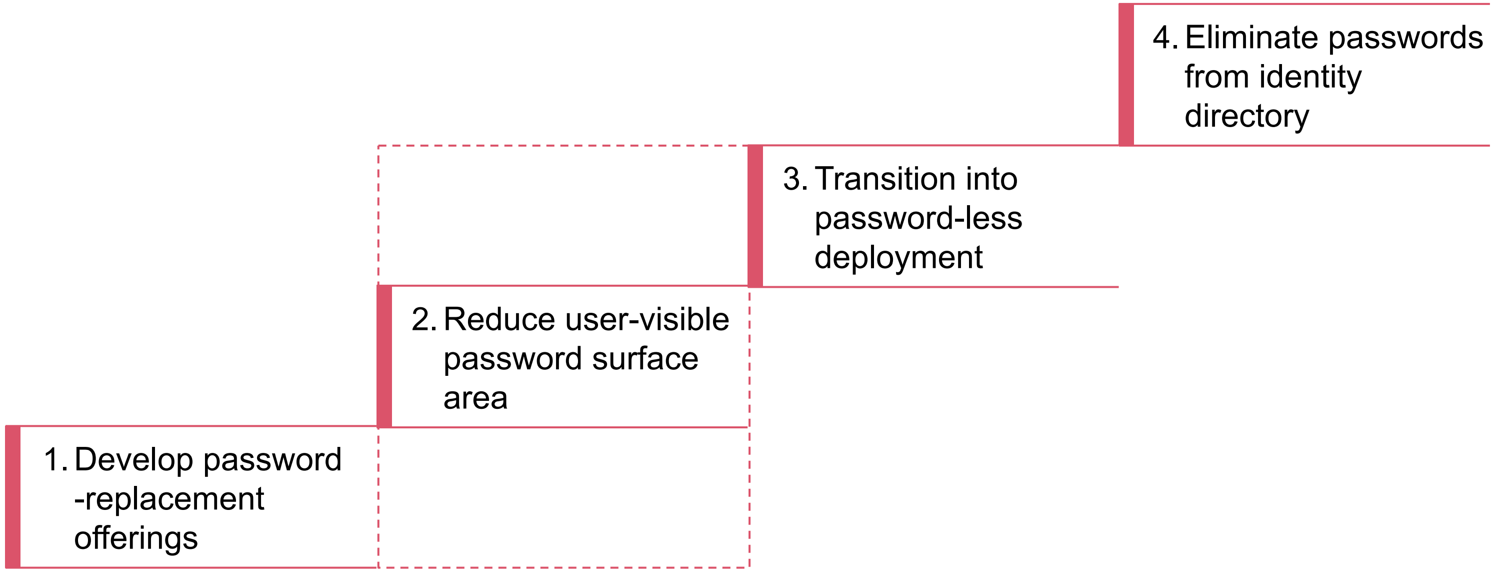


Something you have

Something you know

Something you are

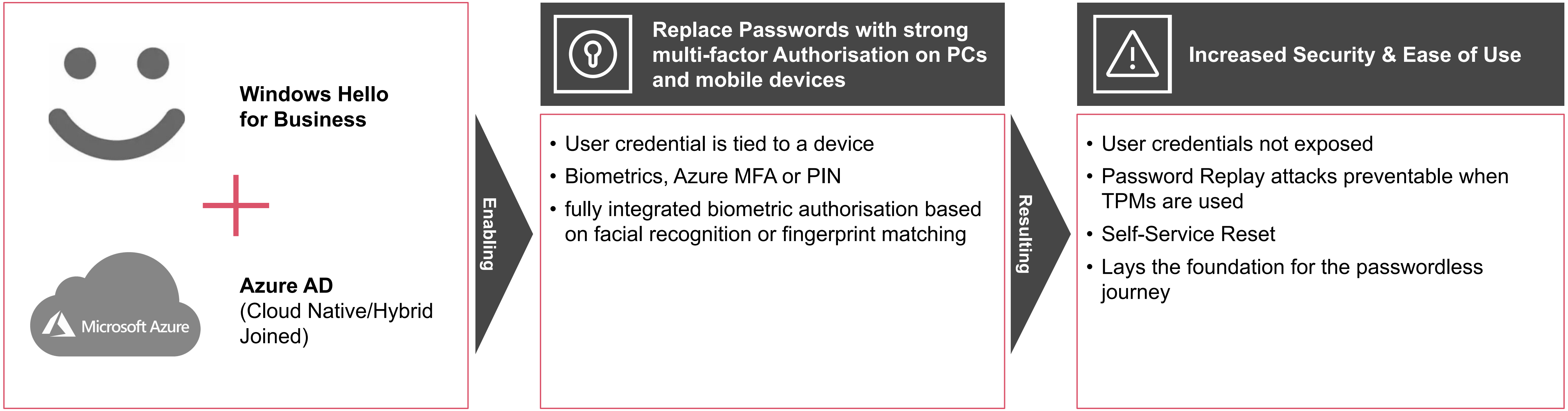
- The solution removes centralised user passwords from credential caches and their transmission over the network
- Simplify Authentication - Leverage Biometrics, FIDO2 or PIN
- Apply conditional access policies to elevate security requirements when needed
- Expand integrations & reduce password usage through Integrated Windows Authentication & Single Sign On
- Leverage your existing IT Infrastructure, reducing spend, increasing value.



1. Develop password -replacement offerings
2. Reduce user-visible password surface area
3. Transition into password-less deployment
4. Eliminate passwords from identity directory

The immediate opportunity

Invest strategically to drive secure access to applications & reduce Tier-0 IT spends



Windows Hello for Business

+

Azure AD (Cloud Native/Hybrid Joined)

Enabling

Replace Passwords with strong multi-factor Authorisation on PCs and mobile devices

- User credential is tied to a device
- Biometrics, Azure MFA or PIN
- fully integrated biometric authorisation based on facial recognition or fingerprint matching

Resulting

Increased Security & Ease of Use

- User credentials not exposed
- Password Replay attacks preventable when TPMs are used
- Self-Service Reset
- Lays the foundation for the passwordless journey

Solution components

Windows Hello for Business can leverage existing IT Infrastructure, reducing disruption and change needed

Identity Providers

Enabling a modern Identity Provider like Azure AD is a key part of the digital transformation of an organisation. PwC's integration enables Windows Hello for Business for Enterprises that have integrated Azure AD with their corporate AD

PKI Infrastructure

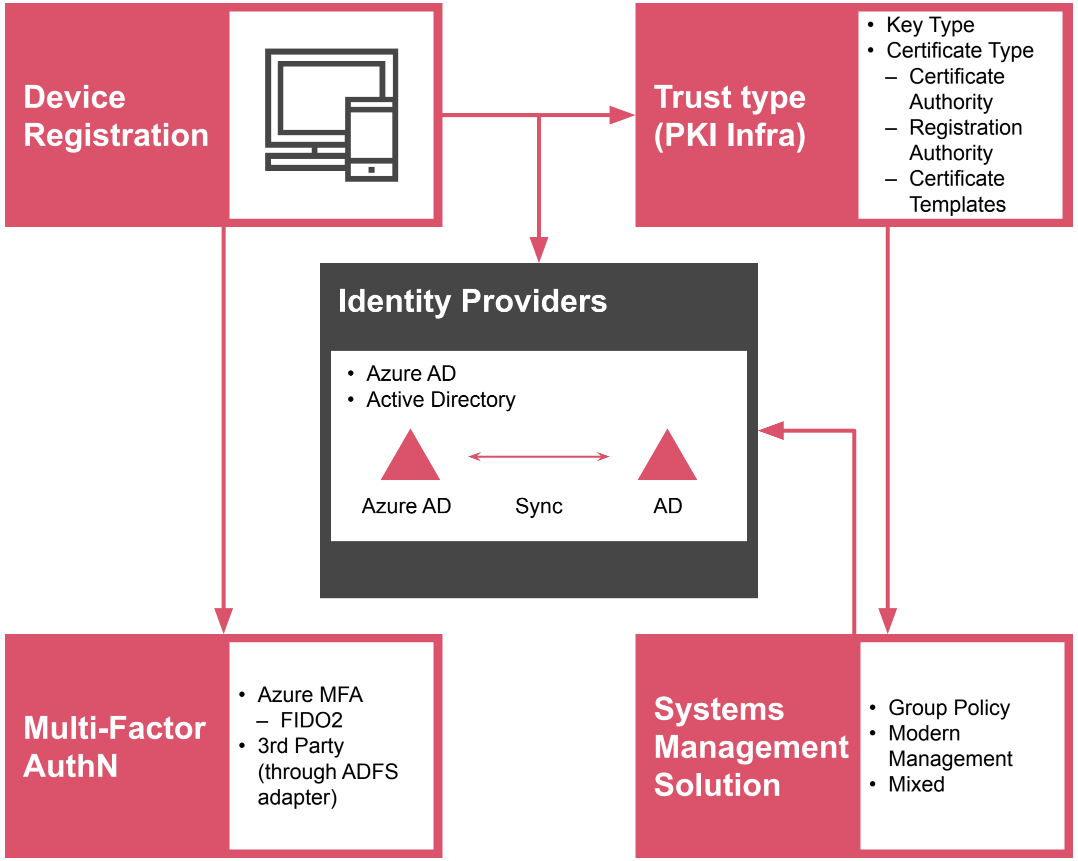
End-users in the organization are required to register their devices and set up their access credentials as a key on that device. Windows Hello for Business supports a key based and a certificate based authentication, allowing enterprises to leverage their existing PKI investments to provide the required encryption & security

Azure AD Device Join

To deploy hybrid certificate trust, enterprises need their domain joined devices to register to Azure Active Directory. Just as a computer has an identity in Active Directory, that same computer has needs an identity in the cloud. This ensures that only approved computers are used with that Azure Active Directory. Each computer registers its identity in Azure Active Directory.

Multi Factor Authentication

The provisioning process lets a user enroll in Windows Hello for Business using their username and password as one factor. but needs a second factor of authentication to complete their authentication



Device Registration

Trust type (PKI Infra)
- Key Type
- Certificate Type
  - Certificate Authority
  - Registration Authority
  - Certificate Templates

Identity Providers
- Azure AD
- Active Directory

Multi-Factor AuthN
- Azure MFA
  - FIDO2
- 3rd Party (through ADFS adapter)

Systems Management Solution
- Group Policy
- Modern Management
- Mixed

How Windows Hello works

Windows Hello for Business can leverage existing IT Infrastructure, reducing disruption and change needed

Device Registration

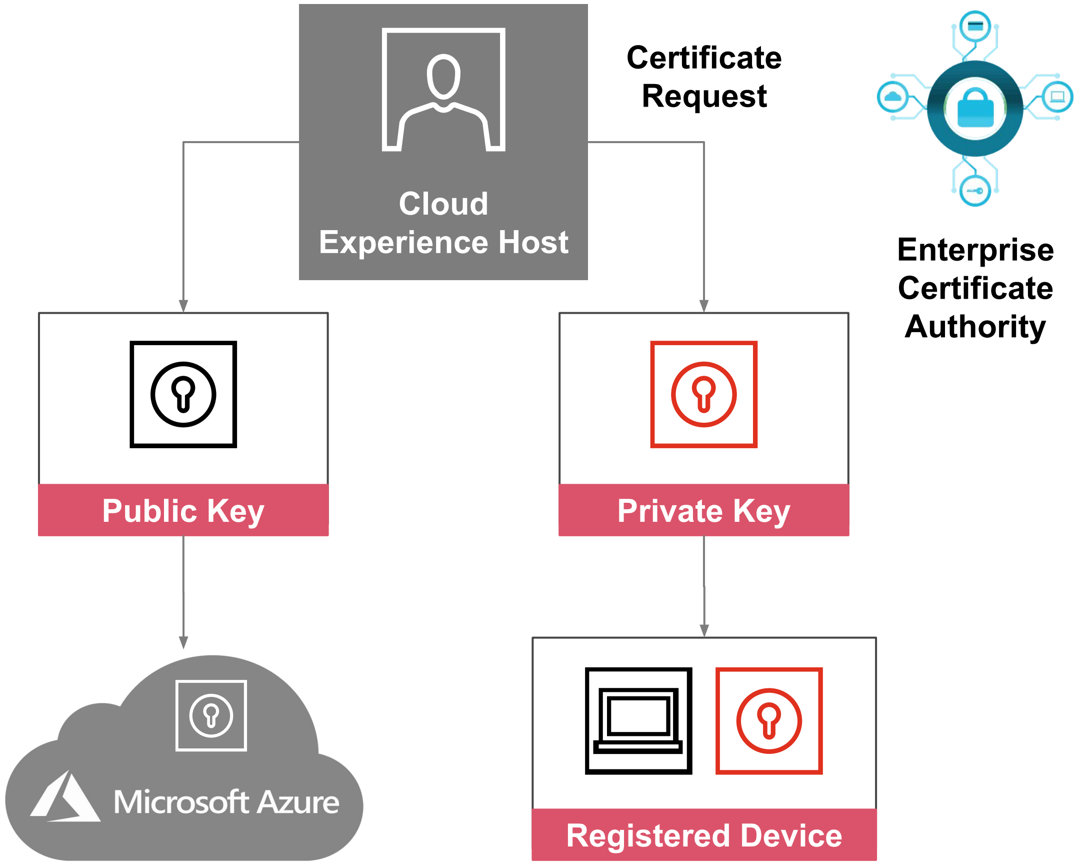
A device key (key-pair, pub & priv keys) is created on the host and a cert request is issued to Azure AD, once Azure DRS validates the information, it creates a Device ID and Certificate. It registers the device and sends the device ID & certificate back for it to use during future authentication requests.

Provisioning

After validating the device registered, the user enrolls a new, strong, two-factor credential for passwordless authentication (Biometric/FIDO2). After enrollment, and a backup pin is created, a business key-pair is generated. On successful validation of the current session, Azure writes the key information to the user record. A key ID is returned back for use during future authentication requests

Certification Trust Deployment

In the case of a certification Trust Deployment approach, the key ID generated during the provisioning step. A PKCS#10 certificate request is using the key is created and sent to the certificate registration authority. The certificate authority validates the key in the request matches values present in Azure for the user and then triggers the certification enrollment processes that result in a newly issued certificate installed into the personal store of the user



Passwordless Enablement

Simplify the journey

With PwC and Microsoft, conduct a rapid pilot and finalise your rollout approach for Windows Hello for Business. We will partner and guide your organisation to make informed strategic decisions that align with the future Enterprise Goals.

Your Passwordless Journey with PwC:

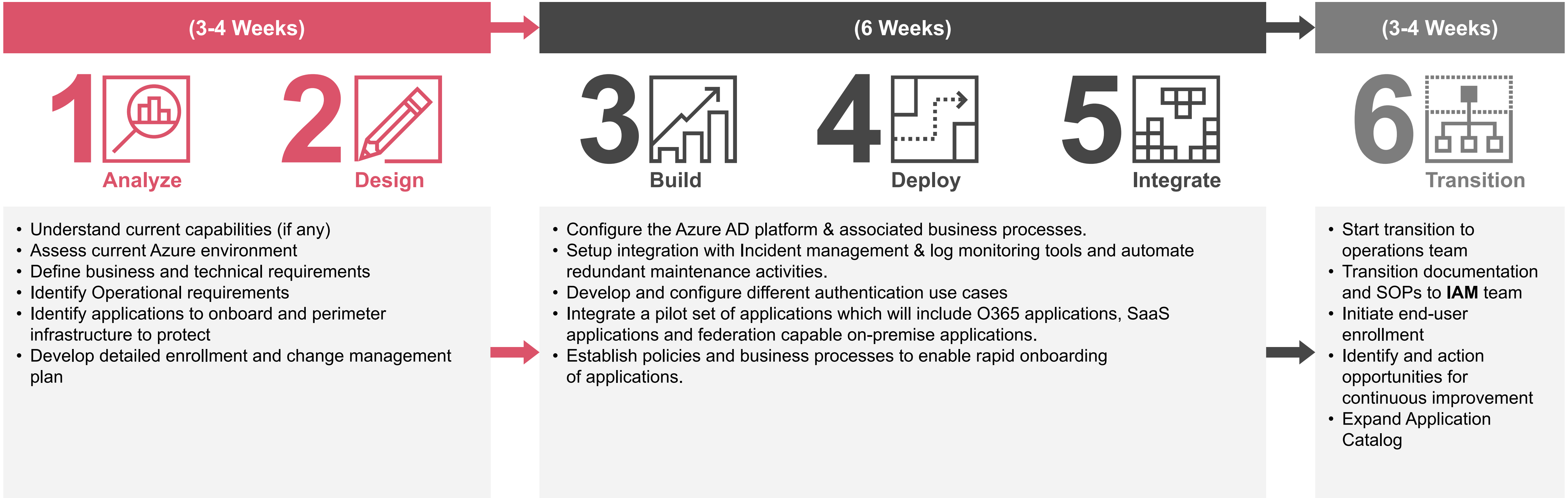
- Quick assessment of your current Microsoft Windows, AD & Azure Landscape
- Determining your Deployment criteria
  - Cloud Native, Hybrid or On-premises
  - Key & Device registration approach
  - Multi-Factor Authentication enablement
  - Workforce Support Use Cases
- Plan & processes for Business Continuity
  - Support Docs, Configuration Guides & Communications Planning
  - Rollout Readiness & Plan
- Accelerators for the Pilot & Rollout

4

Deployment Approach

Our approach – Design & implement a standards based enterprise IAM solution

Combine Microsoft's cybersecurity technologies with PwC's implementation expertise to design and configure a Standards based standalone or hybrid Azure AD solution to provide SSO, MFA and Windows Hello across federation capable On-Premise and SaaS applications (including O365)



(3-4 Weeks)

1 Analyze

2 Design

- Understand current capabilities (if any)
- Assess current Azure environment
- Define business and technical requirements
- Identify Operational requirements
- Identify applications to onboard and perimeter infrastructure to protect
- Develop detailed enrollment and change management plan

(6 Weeks)

3 Build

4 Deploy

5 Integrate

- Configure the Azure AD platform & associated business processes.
- Setup integration with Incident management & log monitoring tools and automate redundant maintenance activities.
- Develop and configure different authentication use cases
- Integrate a pilot set of applications which will include O365 applications, SaaS applications and federation capable on-premise applications.
- Establish policies and business processes to enable rapid onboarding of applications.

(3-4 Weeks)

6 Transition

- Start transition to operations team
- Transition documentation and SOPs to **IAM** team
- Initiate end-user enrollment
- Identify and action opportunities for continuous improvement
- Expand Application Catalog

Learn more

Contact us to learn more about how you can transform your cybersecurity operations

Haitham Al-Jowhari
Partner
Haitham.Al-Jowhari@pwc.com
+971 56676 1146

James Toulman
Director, Cloud Services
James.Toulman@pwc.com
+971 56227 1811

Thank you

pwc.com