AZURE 104

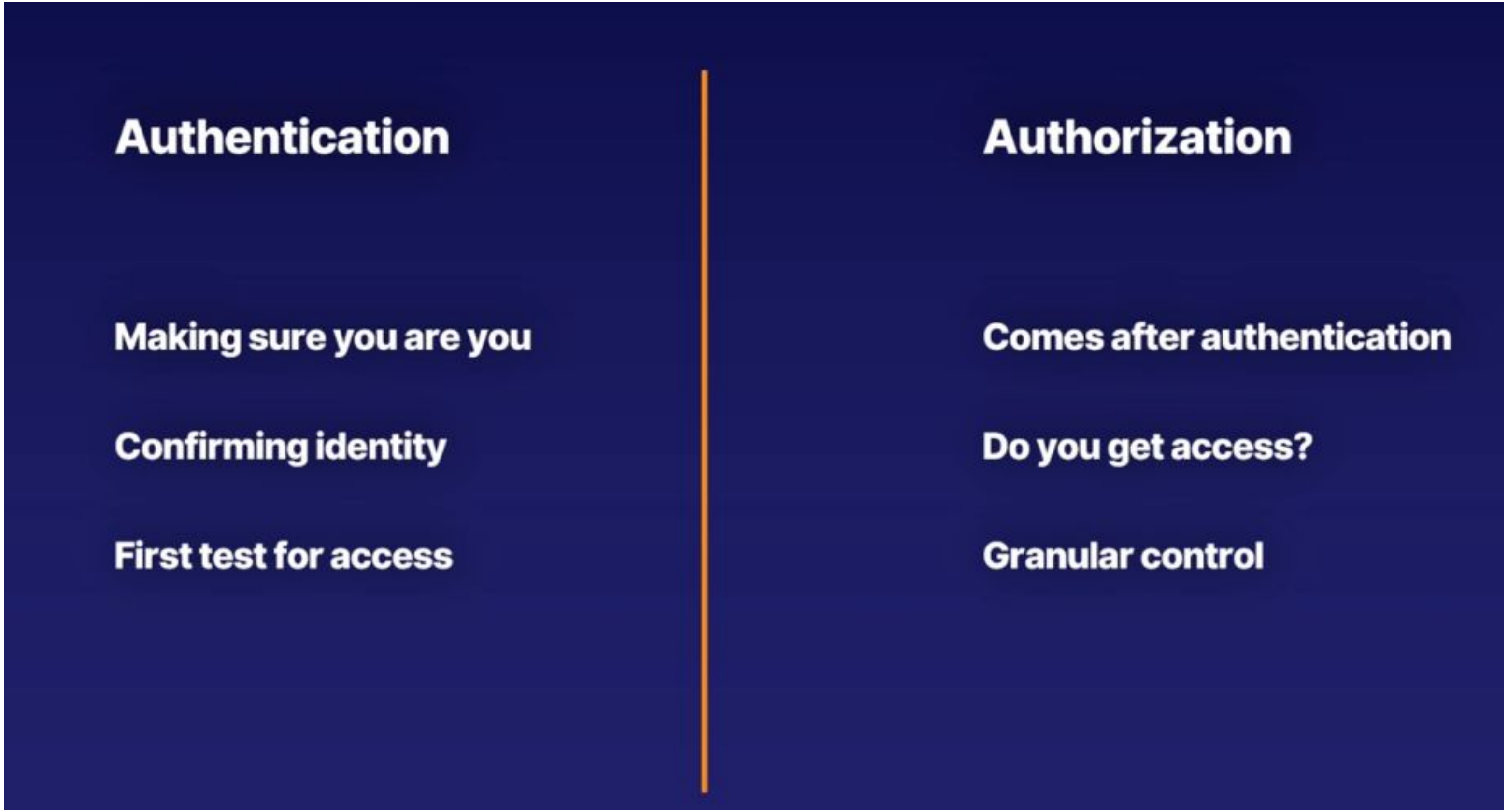
Azure Authentication and Authorization

Plan

1. **Authentication and Authorization**
2. **Azure Active Directory**
3. **Identity and Access Management**
4. **Multi-Factor Authentication**
5. **Azure Seamless Single Sign-On**
6. **Hybrid Identity**

Authentication and Authorization

Identity Services | Authentication & Authorization



Authentication

Making sure you are you

Confirming identity

First test for access

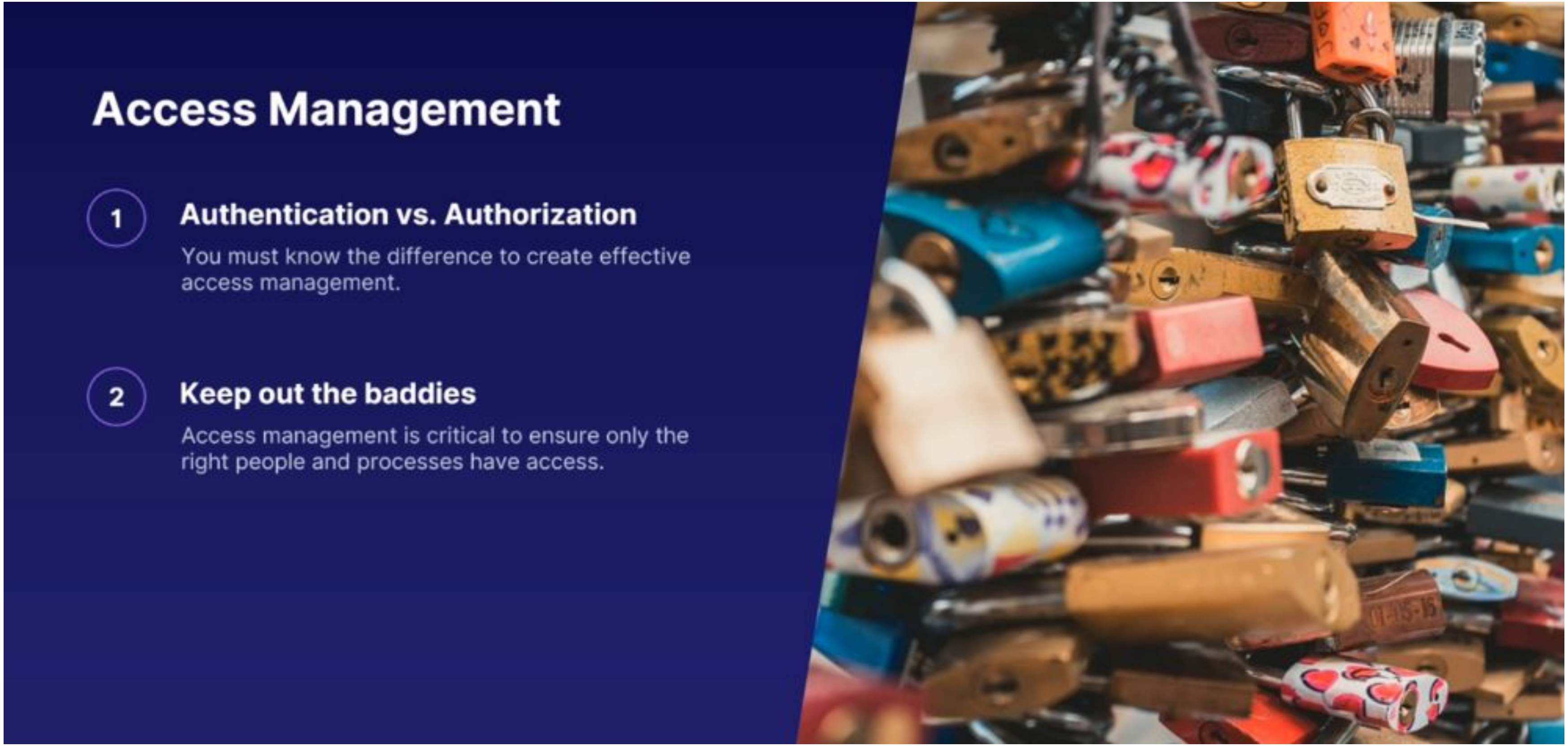
Authorization

Comes after authentication

Do you get access?

Granular control

Identity Services



Access Management

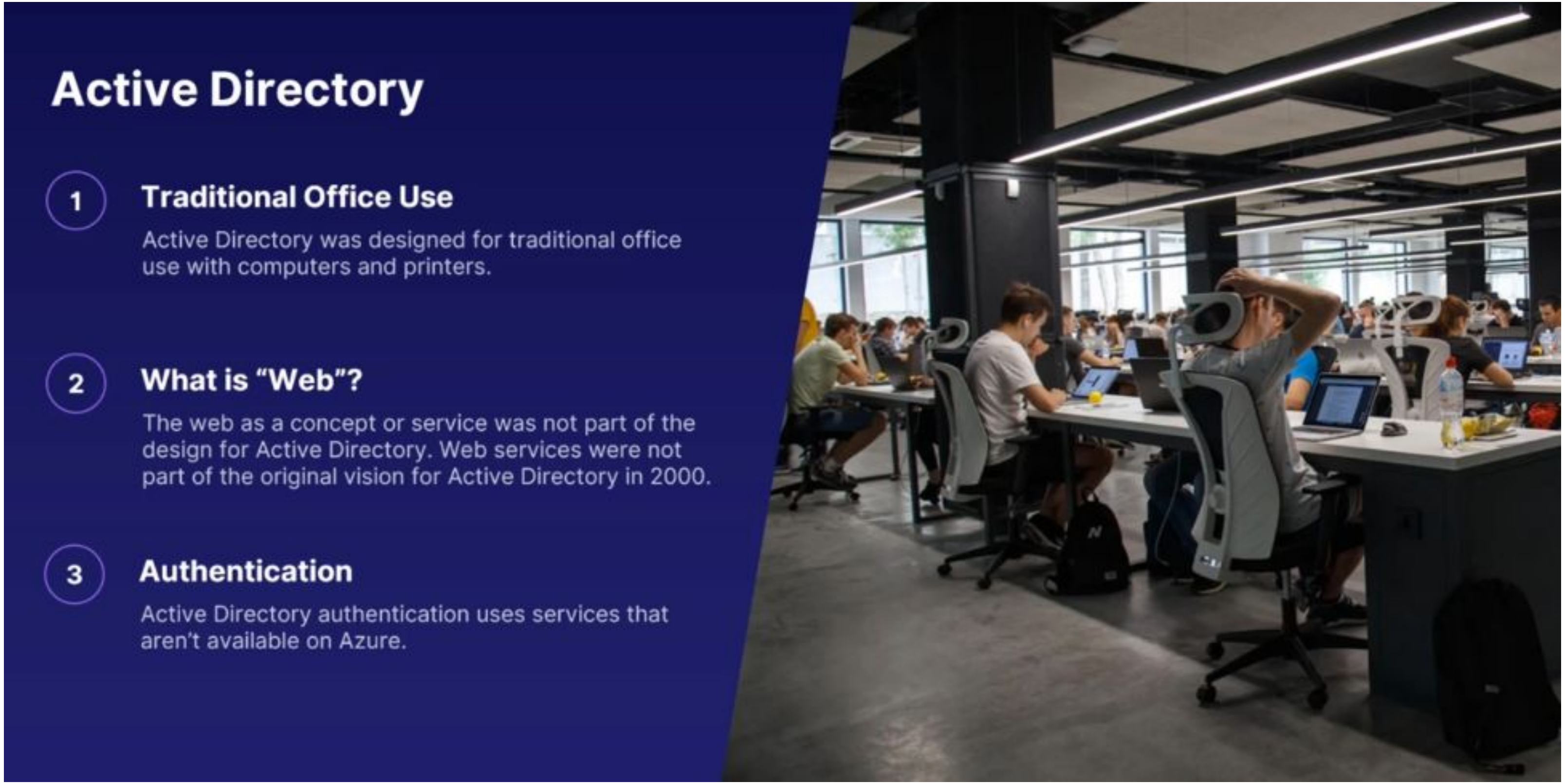
1 **Authentication vs. Authorization**

You must know the difference to create effective access management.

2 **Keep out the baddies**

Access management is critical to ensure only the right people and processes have access.

Azure Active Directory



Active Directory

1. **Traditional Office Use**

   Active Directory was designed for traditional office use with computers and printers.

2. **What is "Web"?**

   The web as a concept or service was not part of the design for Active Directory. Web services were not part of the original vision for Active Directory in 2000.

3. **Authentication**

   Active Directory authentication uses services that aren't available on Azure.

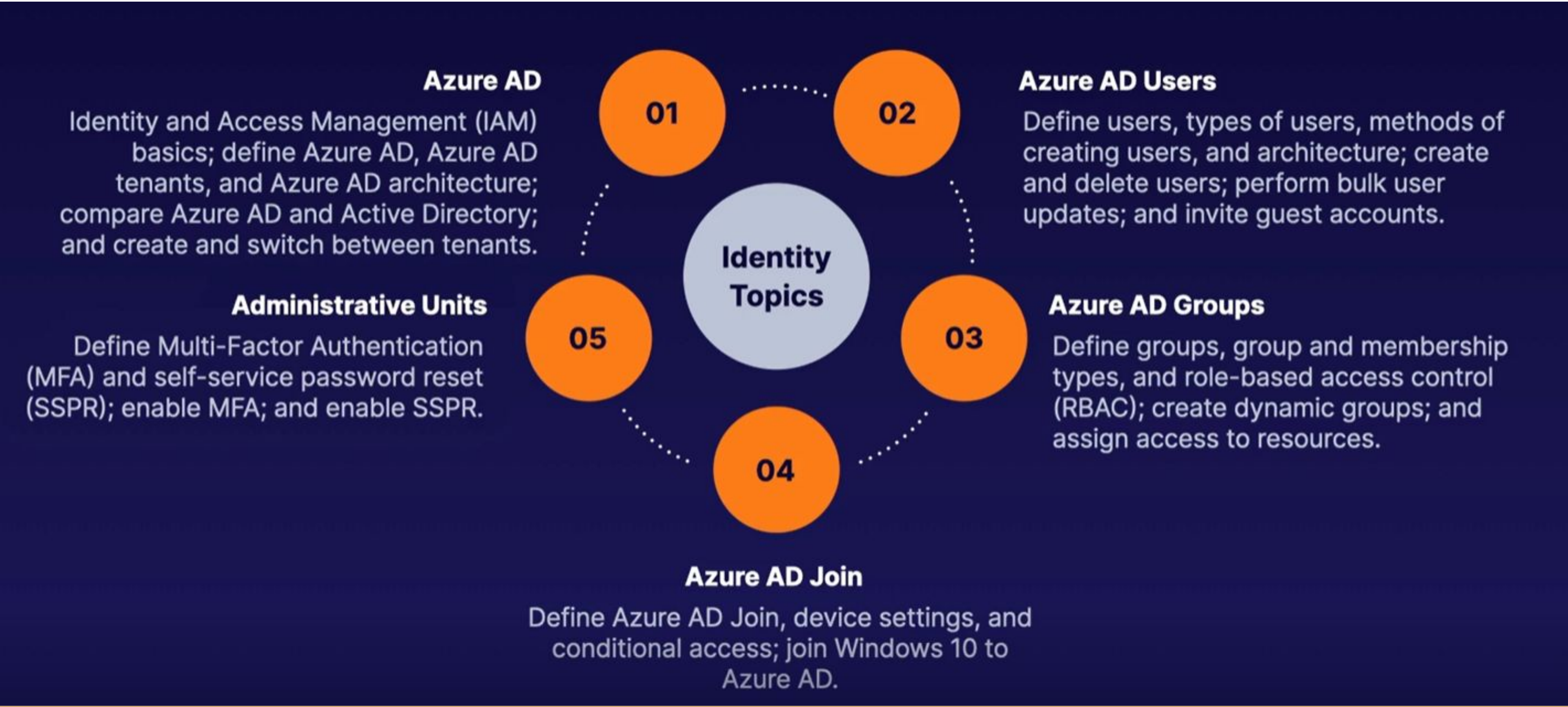
Azure Active Directory

- Microsoft introduced Active Directory in the year 2000 which to this day is one of the best products from its stable.
- Any Enterprise with Windows servers would be running the Domain Controllers in a **Domain/Tree/Forest** organization setup with multiple DCs playing different roles **(called FSMO – Flexible single master operation)** and in multiple locations for load balancing and reducing latency and increasing fault tolerance.
- Before this, Microsoft had NT4 where there was a single PDC (Primary Domain Controller) backed by a BDC (Backup Domain Controller) to provide Enterprise Identity Management.

Azure Active Directory

- Windows 2000 and beyond uses the Active Directory and it uses **LDAP (Lightweight directory access Protocol)/Kerberos** for authentication. Here all resources like computers, printers, etc are all considered objects.
- This concept changed with Azure Directory which like most cloud service providers also uses REST API in the background.
- Any service invoked on the Azure cloud is with REST APIs and this is the foundation for **AAD (Azure Active Directory)**. Therefore, AD on the client premises and AAD on the cloud will not work seamlessly.

Azure Active Directory



Identity Topics

01

Azure AD

Identity and Access Management (IAM) basics; define Azure AD, Azure AD tenants, and Azure AD architecture; compare Azure AD and Active Directory; and create and switch between tenants.

02

Azure AD Users

Define users, types of users, methods of creating users, and architecture; create and delete users; perform bulk user updates; and invite guest accounts.

03

Azure AD Groups

Define groups, group and membership types, and role-based access control (RBAC); create dynamic groups; and assign access to resources.

04

Azure AD Join

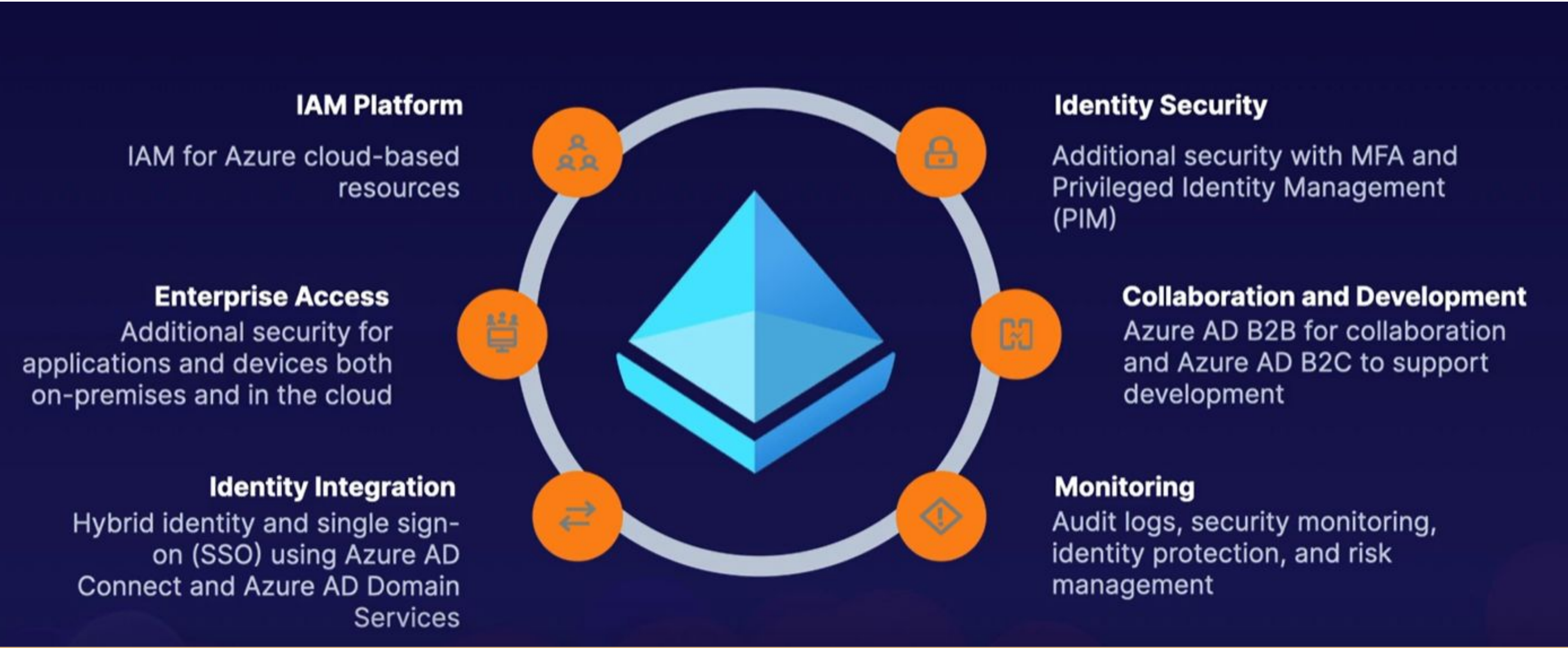
Define Azure AD Join, device settings, and conditional access; join Windows 10 to Azure AD.

05

Administrative Units

Define Multi-Factor Authentication (MFA) and self-service password reset (SSPR); enable MFA; and enable SSPR.

Azure Active Directory Features



IAM Platform

IAM for Azure cloud-based resources

Enterprise Access

Additional security for applications and devices both on-premises and in the cloud

Identity Integration

Hybrid identity and single sign-on (SSO) using Azure AD Connect and Azure AD Domain Services

Identity Security

Additional security with MFA and Privileged Identity Management (PIM)

Collaboration and Development

Azure AD B2B for collaboration and Azure AD B2C to support development

Monitoring

Audit logs, security monitoring, identity protection, and risk management

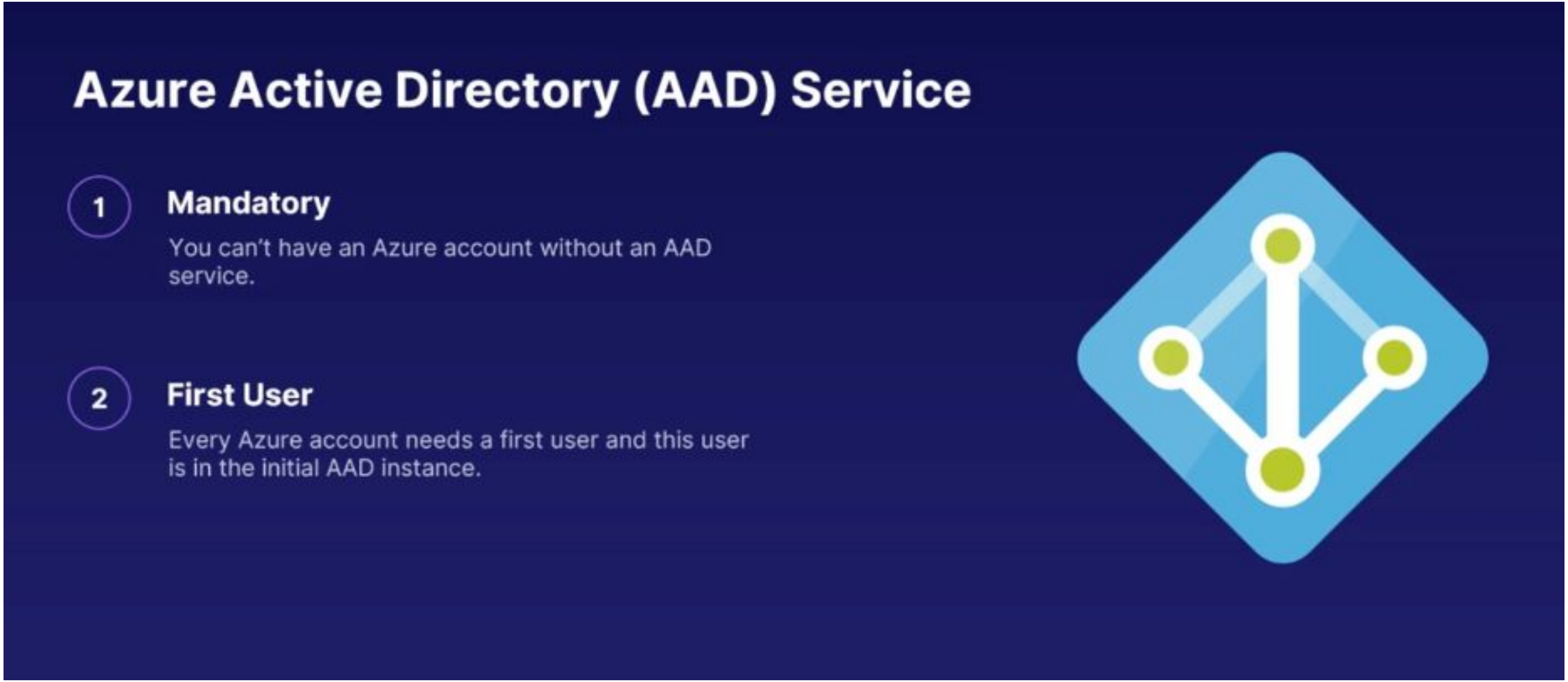
Azure Active Directory

Active Directory
IS NOT
Azure
Active Directory

Active Directory VS Azure Active Directory

Communication	As discussed, AD uses LDAP and AAD uses REST API.
Network Organization	AD uses Forest/Domain/Tree/Organizational Unit (OU) whereas AAD uses users and groups.
Authentication	Cloud based protocols for AD/ AAD uses Kerberos and NTLM
Access Setup	AD uses Admin/data owners and AAD organizes users into groups
Desktops	AD uses GPO (group policy object) and AAD can use Microsoft intune to join desktops

Azure Active Directory



Azure Active Directory (AAD) Service

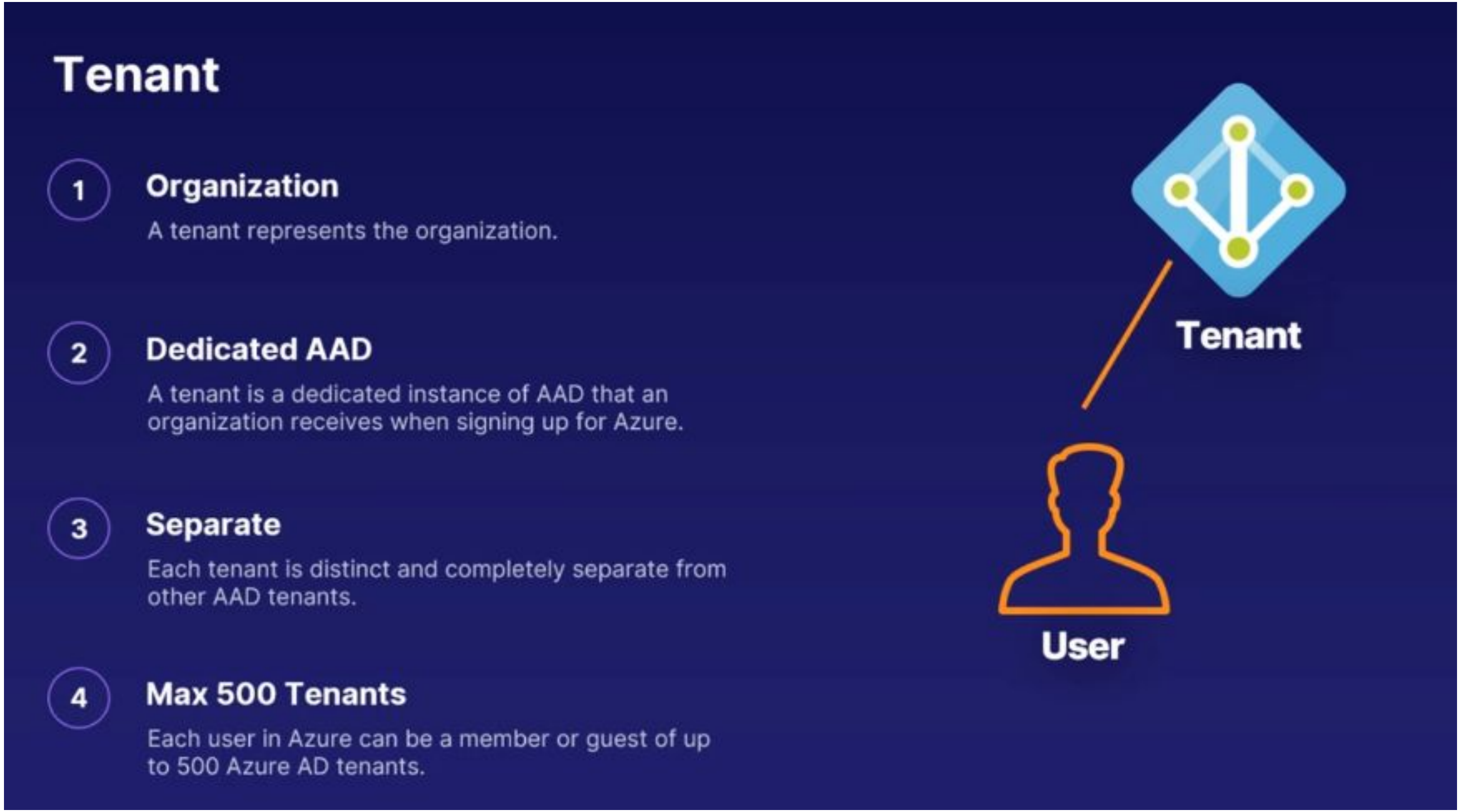
1. **Mandatory**

   You can't have an Azure account without an AAD service.

2. **First User**

   Every Azure account needs a first user and this user is in the initial AAD instance.

Azure Active Directory



Tenant

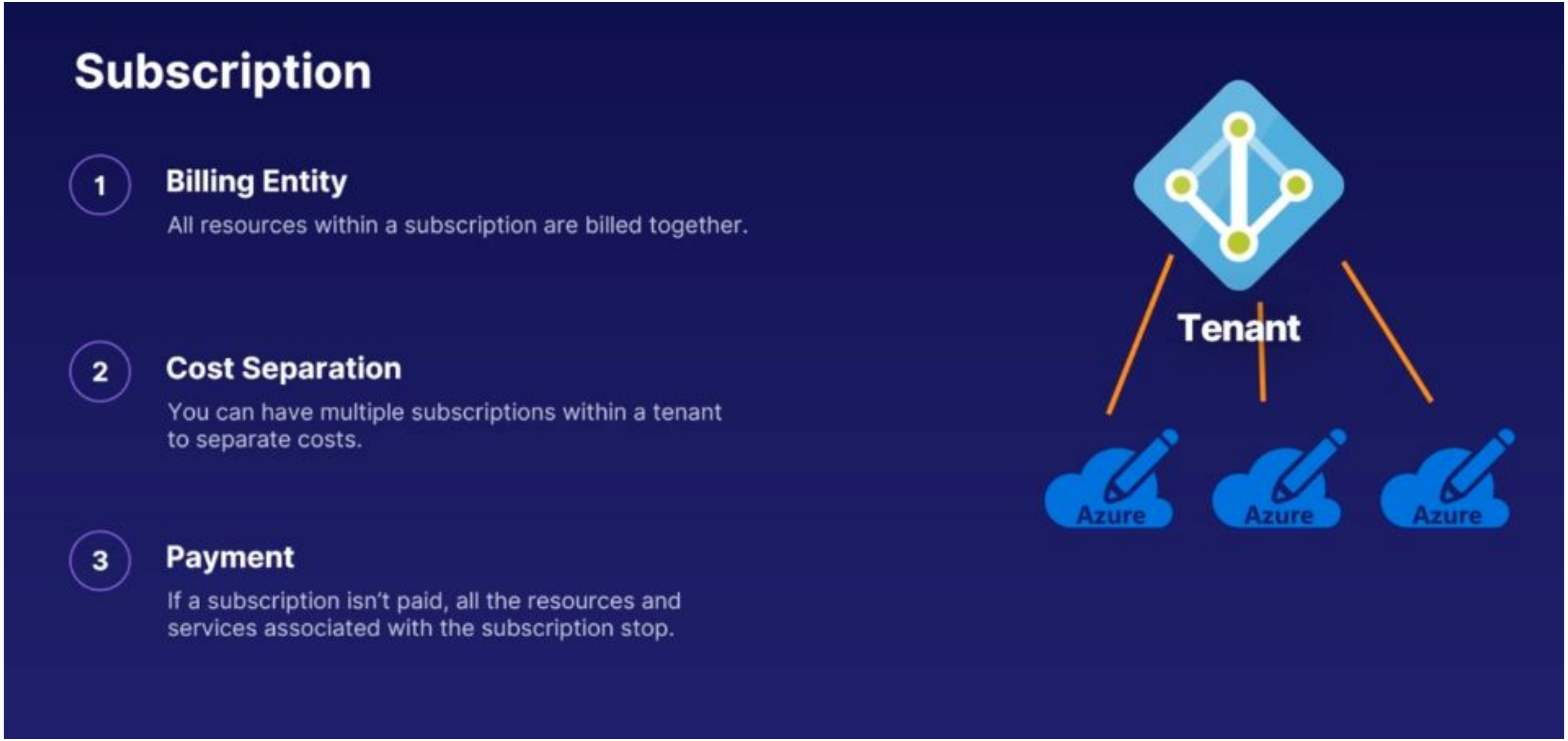
1. **Organization**
   A tenant represents the organization.

2. **Dedicated AAD**
   A tenant is a dedicated instance of AAD that an organization receives when signing up for Azure.

3. **Separate**
   Each tenant is distinct and completely separate from other AAD tenants.

4. **Max 500 Tenants**
   Each user in Azure can be a member or guest of up to 500 Azure AD tenants.

Azure Active Directory



Subscription

1 **Billing Entity**

All resources within a subscription are billed together.

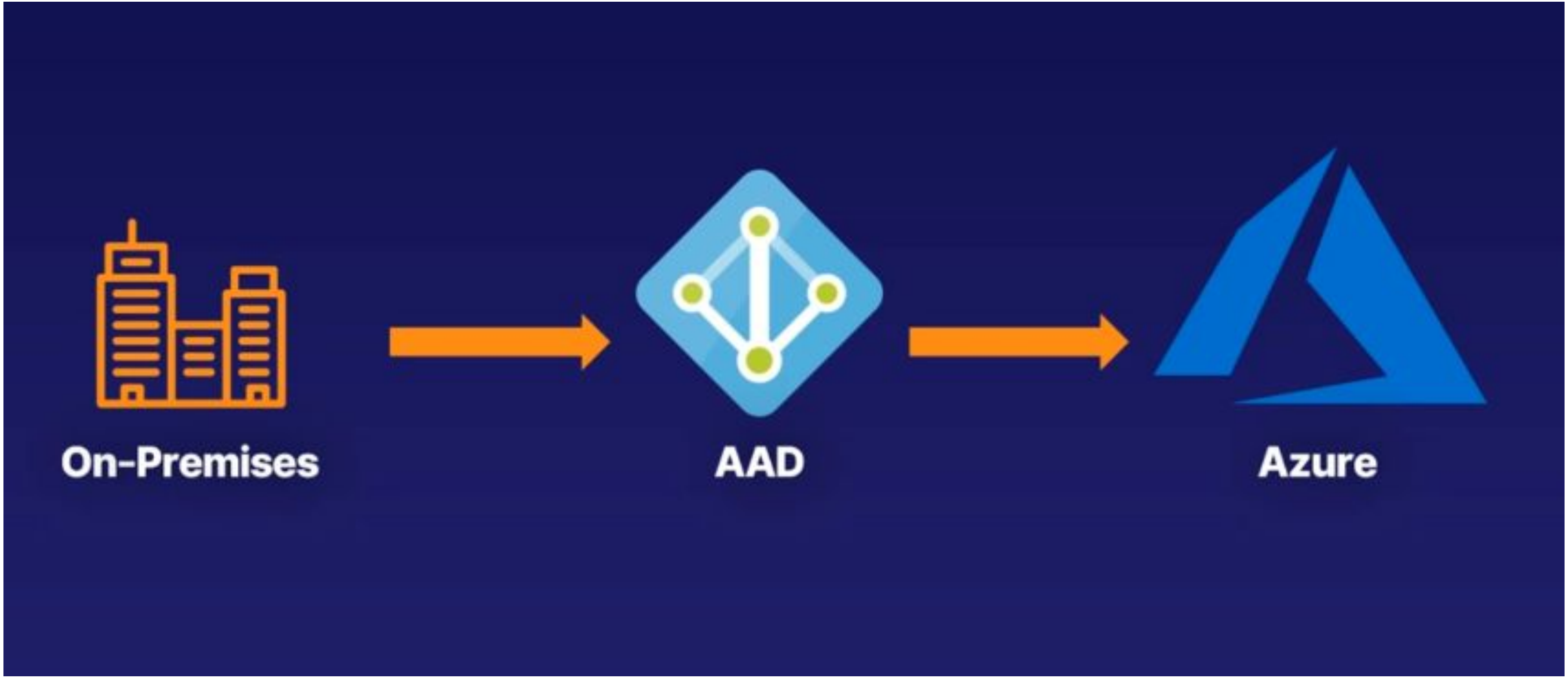
2 **Cost Separation**

You can have multiple subscriptions within a tenant to separate costs.

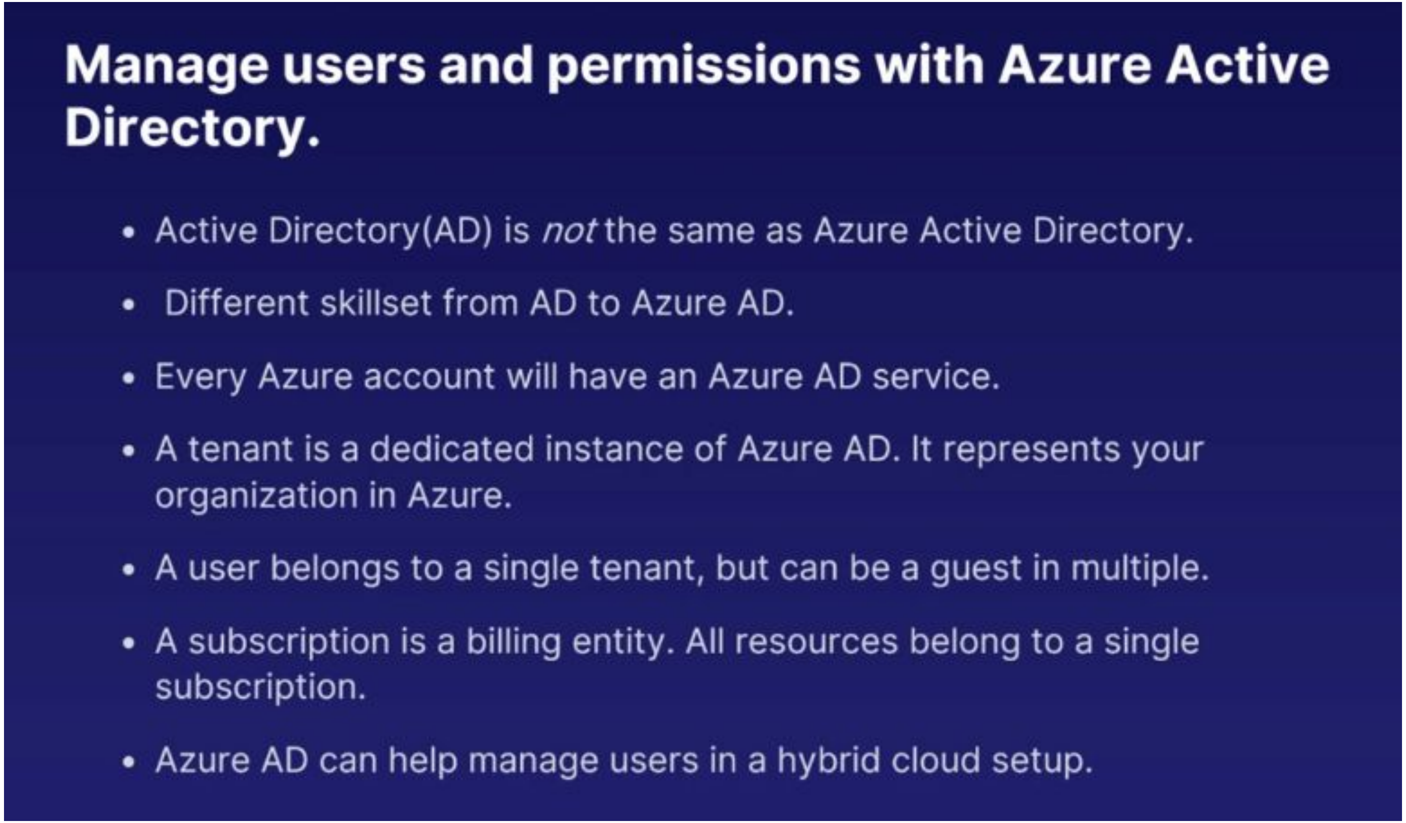
3 **Payment**

If a subscription isn't paid, all the resources and services associated with the subscription stop.

Azure Active Directory | Hybrid cloud provider



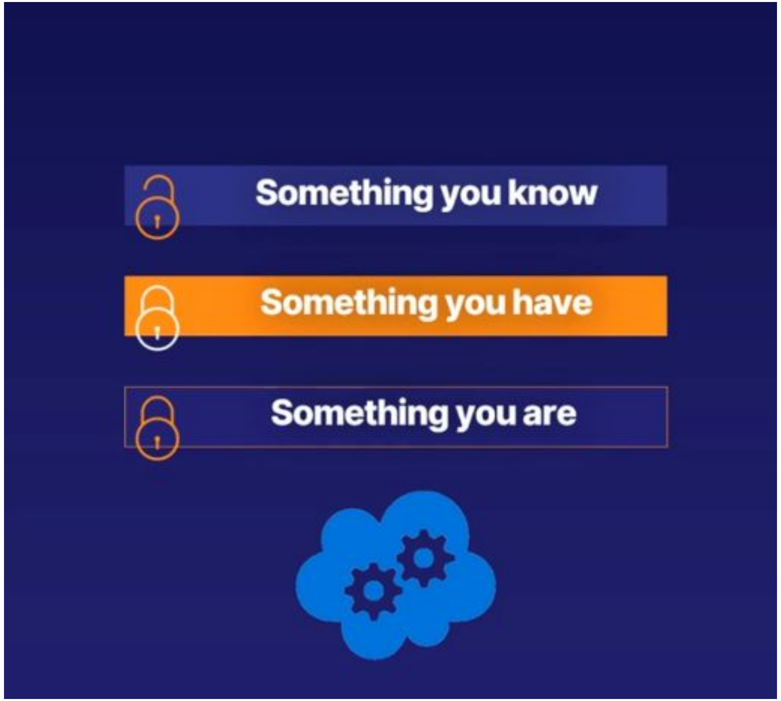
Azure Active Directory | Hybrid cloud provider



Manage users and permissions with Azure Active Directory.

- Active Directory(AD) is *not* the same as Azure Active Directory.
- Different skillset from AD to Azure AD.
- Every Azure account will have an Azure AD service.
- A tenant is a dedicated instance of Azure AD. It represents your organization in Azure.
- A user belongs to a single tenant, but can be a guest in multiple.
- A subscription is a billing entity. All resources belong to a single subscription.
- Azure AD can help manage users in a hybrid cloud setup.

Multifactor Authentication

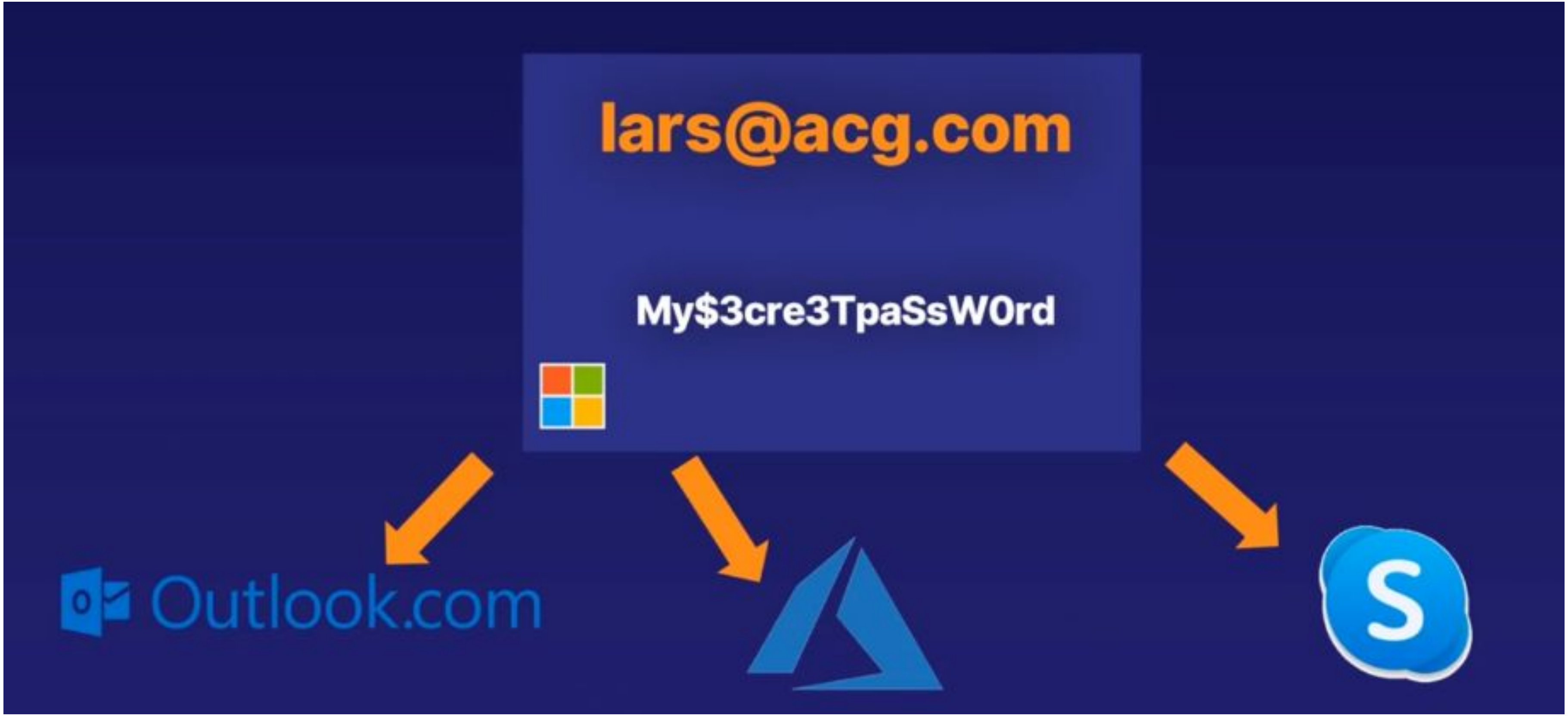


Multifactor Authentication

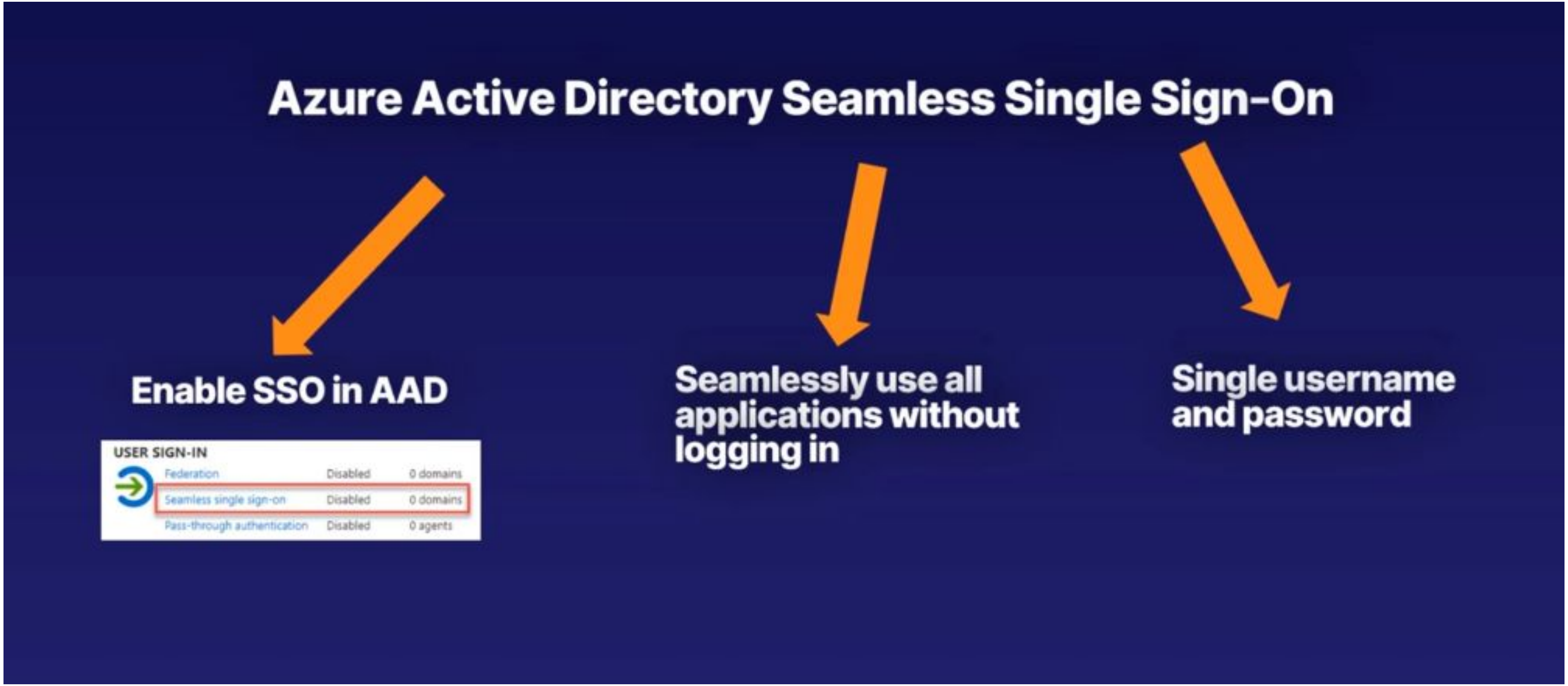
jane.smith@outlook.com
****
3757

Single Sign-on

Single Sign-on



Single Sign-on | Azure SSO



Azure Active Directory Seamless Single Sign-On

Enable SSO in AAD

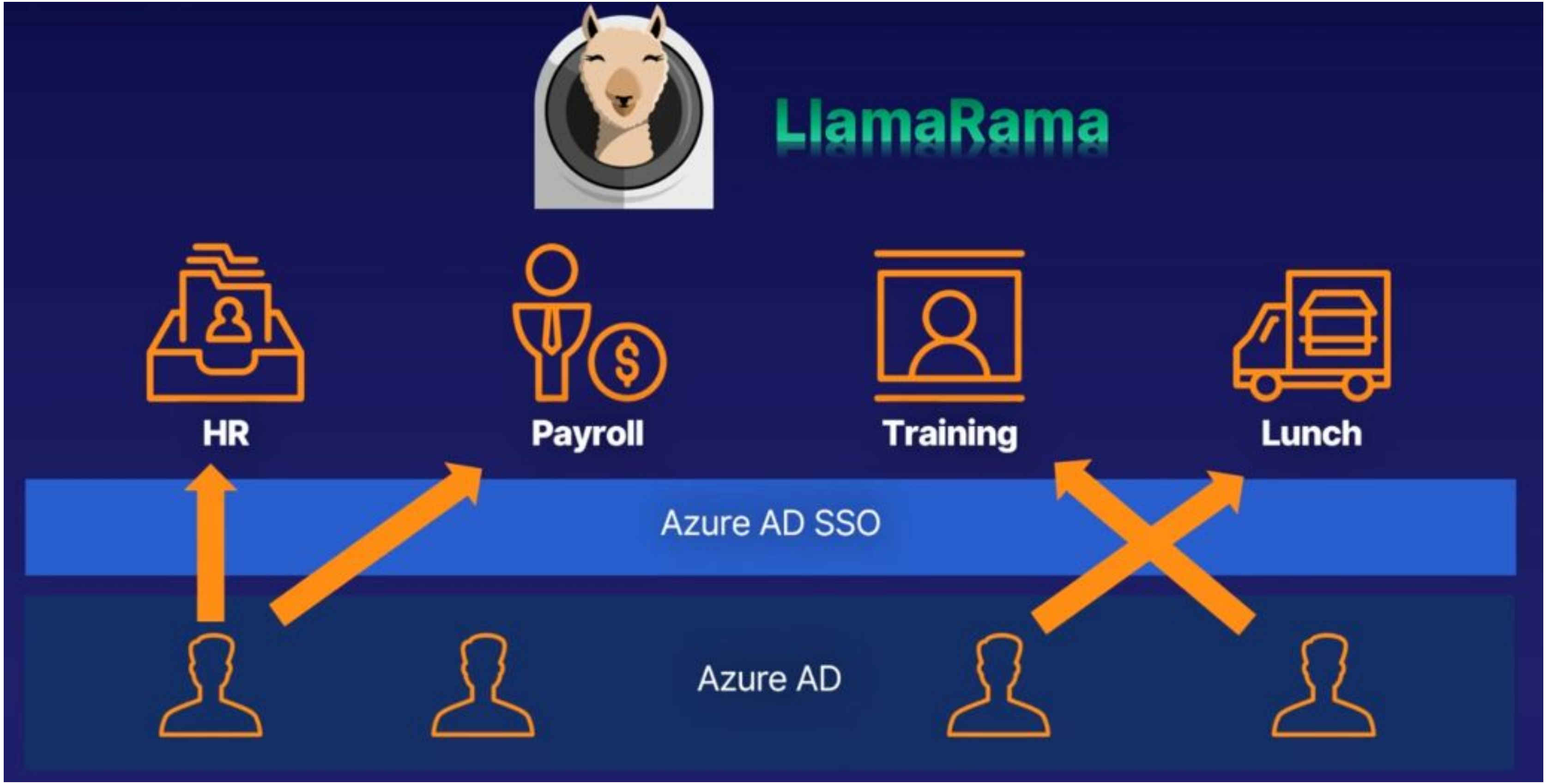
USER SIGN-IN

Federation	Disabled	0 domains
Seamless single sign-on	Disabled	0 domains
Pass-through authentication	Disabled	0 agents

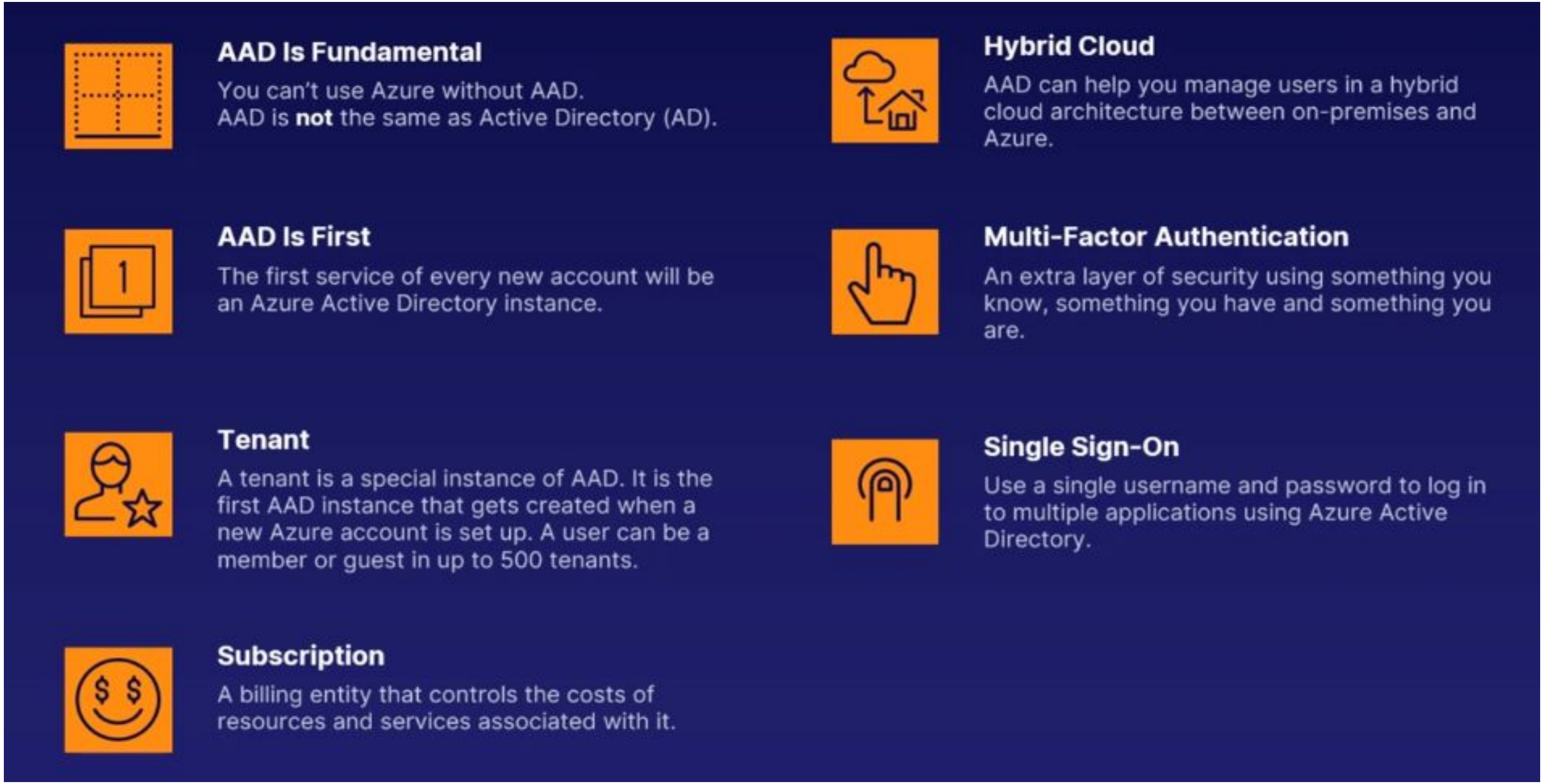
Seamlessly use all applications without logging in

Single username and password

Single Sign-on



Summary



AAD Is Fundamental

You can't use Azure without AAD.
AAD is **not** the same as Active Directory (AD).

AAD Is First

The first service of every new account will be an Azure Active Directory instance.

Tenant

A tenant is a special instance of AAD. It is the first AAD instance that gets created when a new Azure account is set up. A user can be a member or guest in up to 500 tenants.

Subscription

A billing entity that controls the costs of resources and services associated with it.

Hybrid Cloud

AAD can help you manage users in a hybrid cloud architecture between on-premises and Azure.

Multi-Factor Authentication

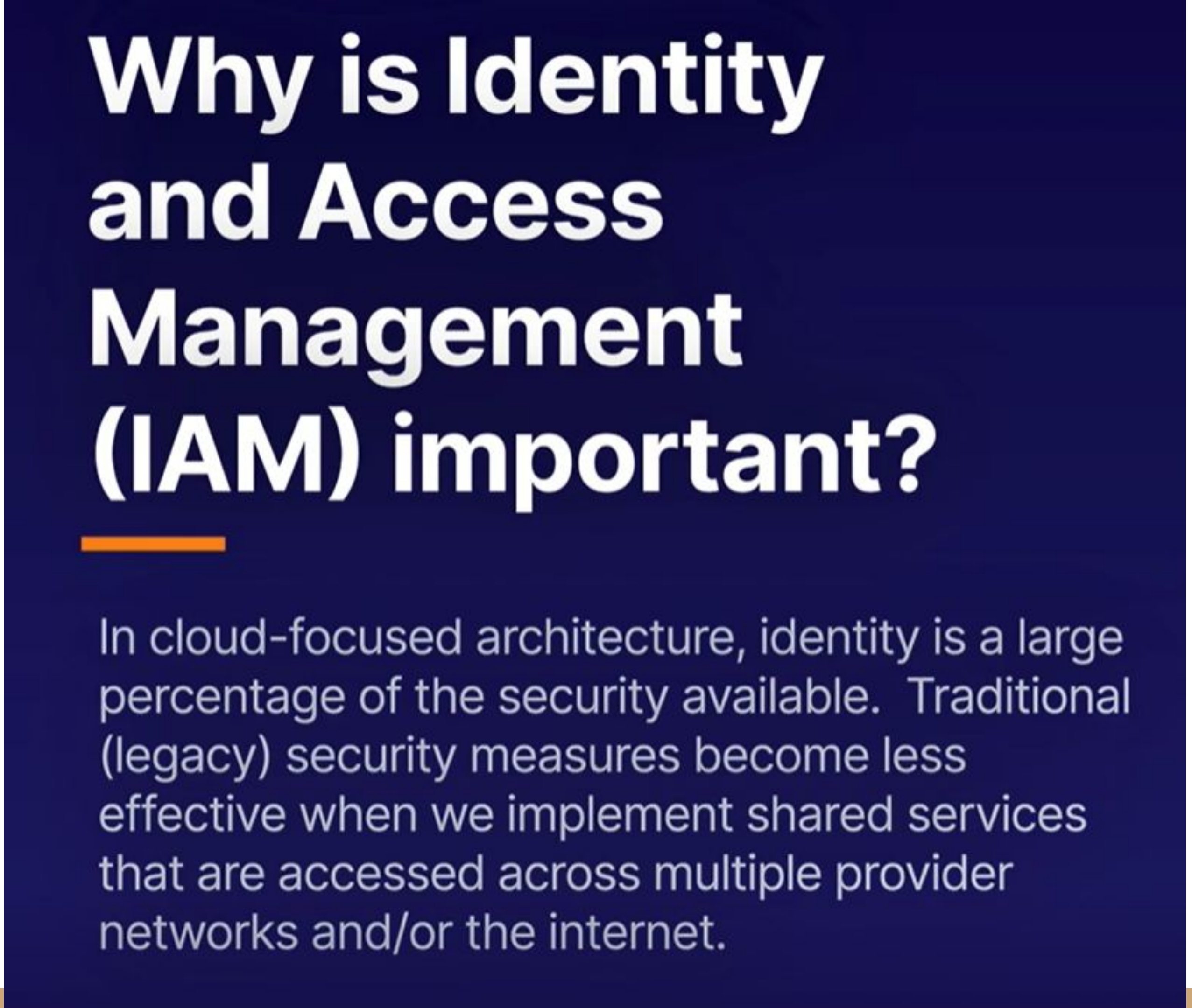
An extra layer of security using something you know, something you have and something you are.

Single Sign-On

Use a single username and password to log in to multiple applications using Azure Active Directory.

Identity and Access Management

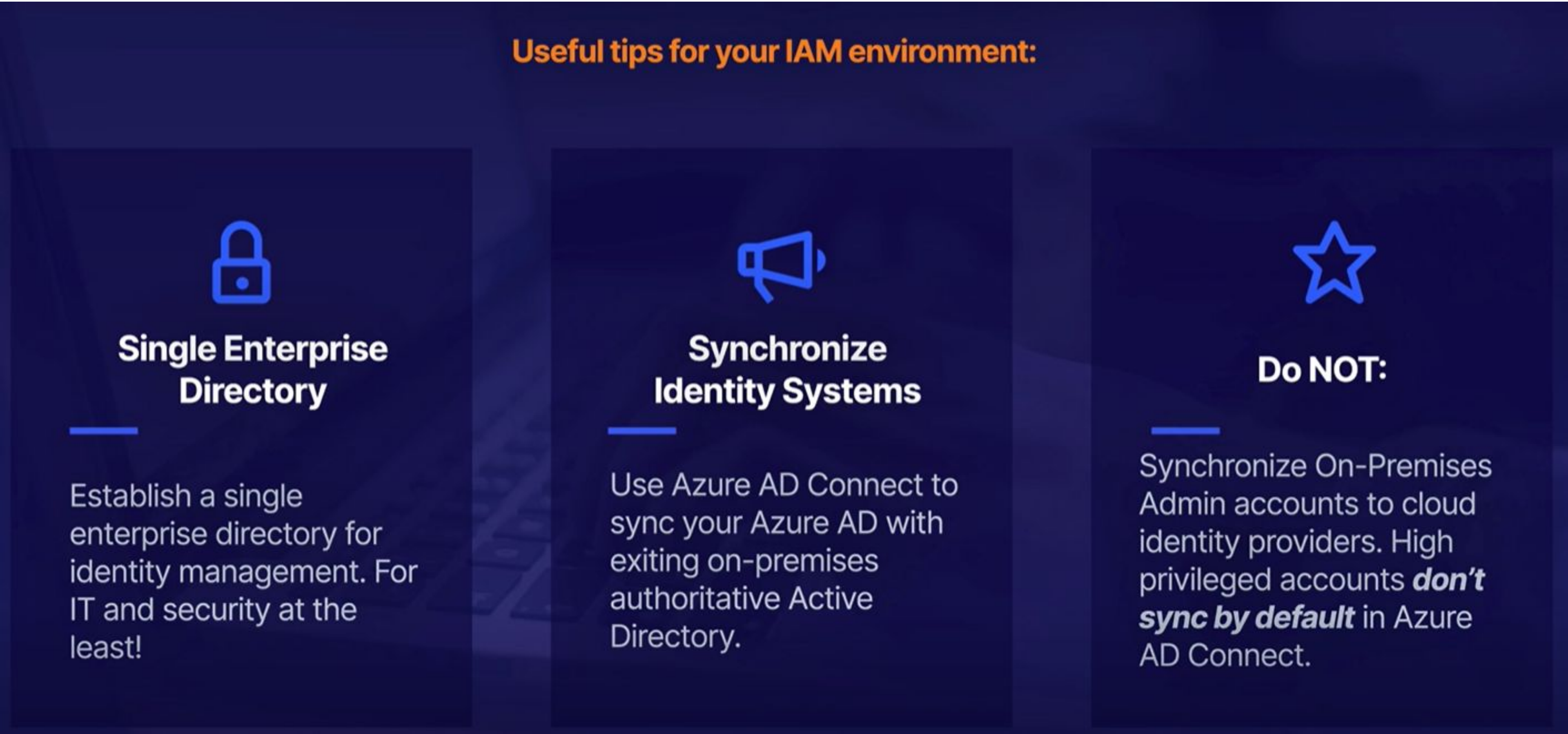
IAM



Why is Identity and Access Management (IAM) important?

In cloud-focused architecture, identity is a large percentage of the security available. Traditional (legacy) security measures become less effective when we implement shared services that are accessed across multiple provider networks and/or the internet.

Identity and Access Management



Useful tips for your IAM environment:

Single Enterprise Directory

Establish a single enterprise directory for identity management. For IT and security at the least!

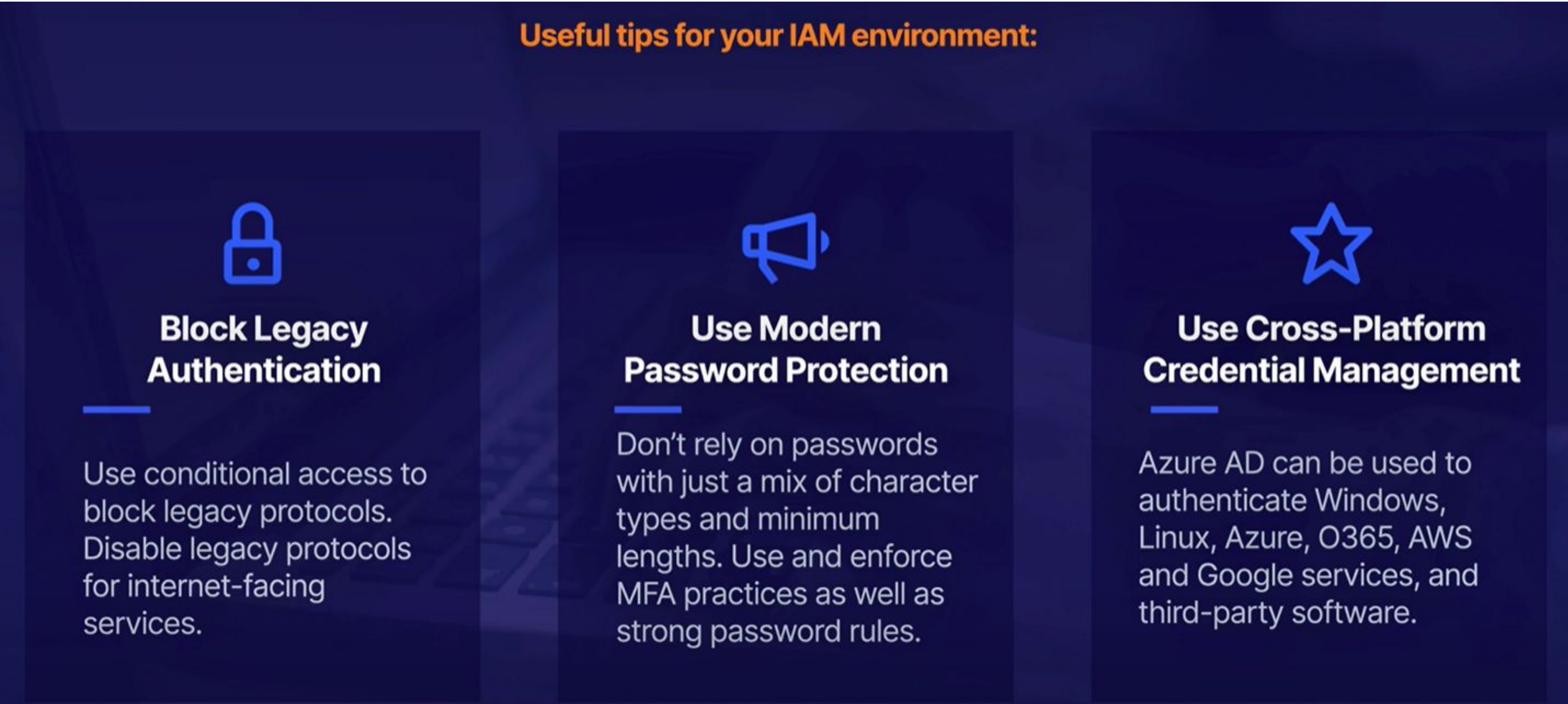
Synchronize Identity Systems

Use Azure AD Connect to sync your Azure AD with exiting on-premises authoritative Active Directory.

Do NOT:

Synchronize On-Premises Admin accounts to cloud identity providers. High privileged accounts ***don't sync by default*** in Azure AD Connect.

Identity and Access Management



Useful tips for your IAM environment:

Block Legacy Authentication

Use conditional access to block legacy protocols. Disable legacy protocols for internet-facing services.

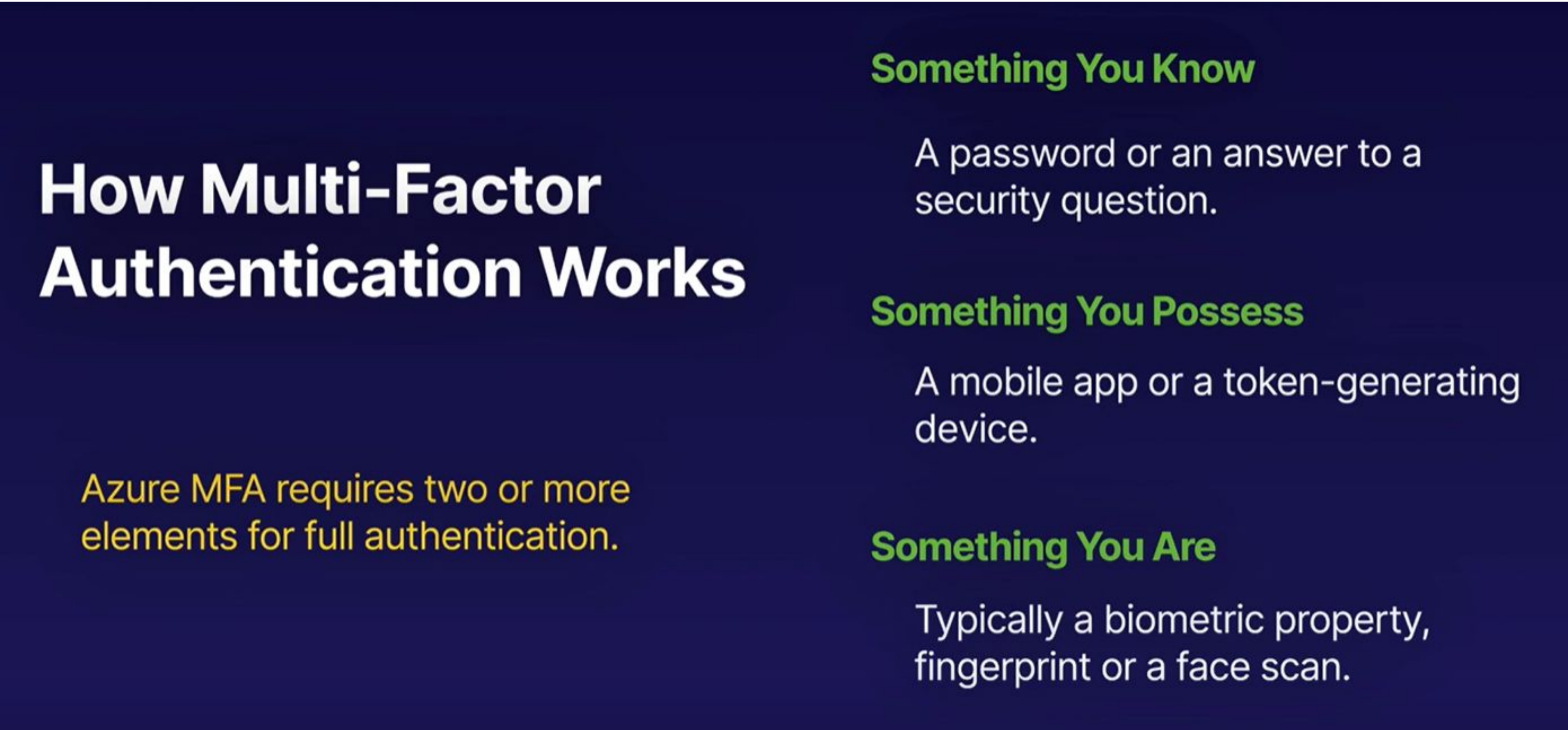
Use Modern Password Protection

Don’t rely on passwords with just a mix of character types and minimum lengths. Use and enforce MFA practices as well as strong password rules.

Use Cross-Platform Credential Management

Azure AD can be used to authenticate Windows, Linux, Azure, O365, AWS and Google services, and third-party software.

Multi-Factor Authentication



How Multi-Factor Authentication Works

Azure MFA requires two or more elements for full authentication.

Something You Know

A password or an answer to a security question.

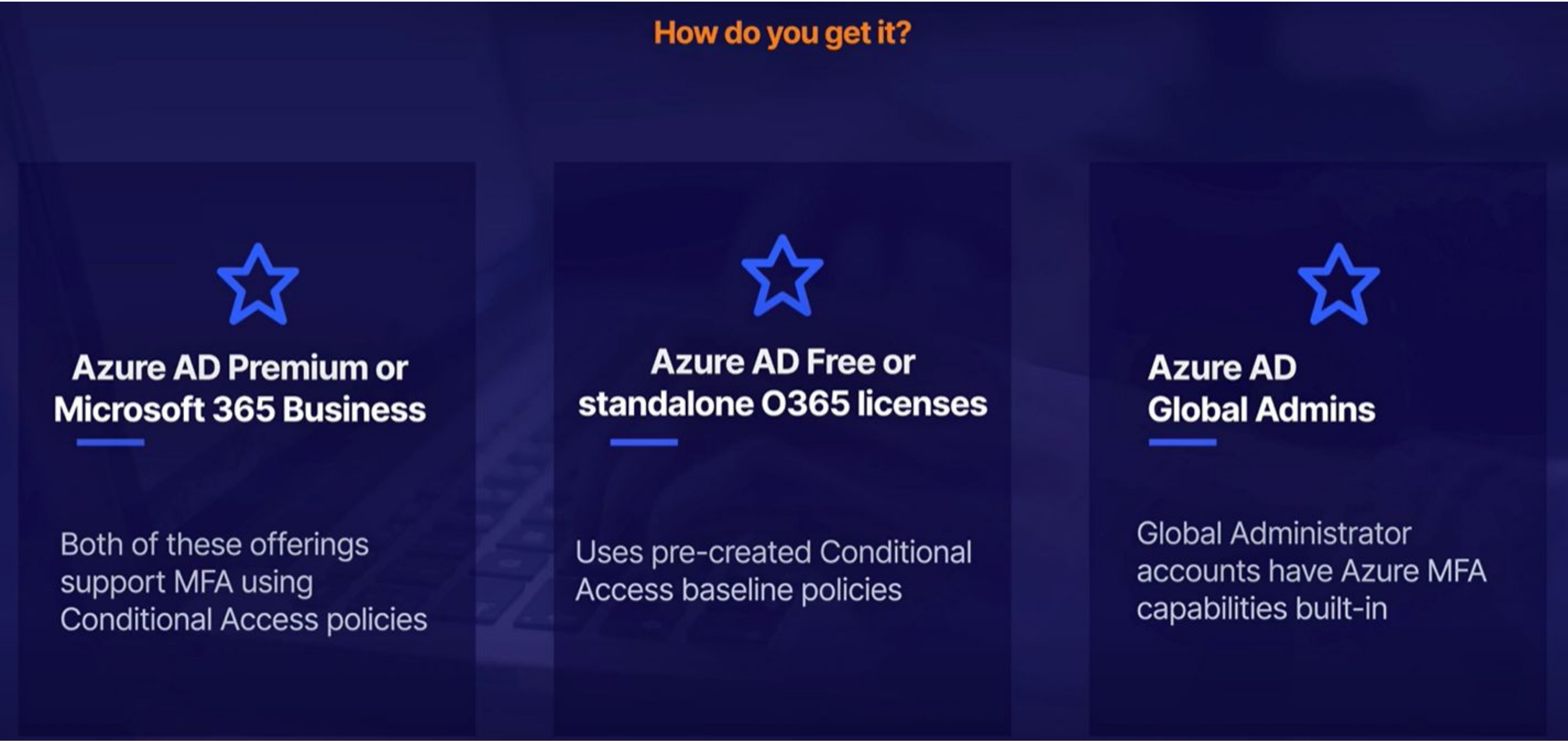
Something You Possess

A mobile app or a token-generating device.

Something You Are

Typically a biometric property, fingerprint or a face scan.

Multi-Factor Authentication



How do you get it?

Azure AD Premium or Microsoft 365 Business

Both of these offerings support MFA using Conditional Access policies

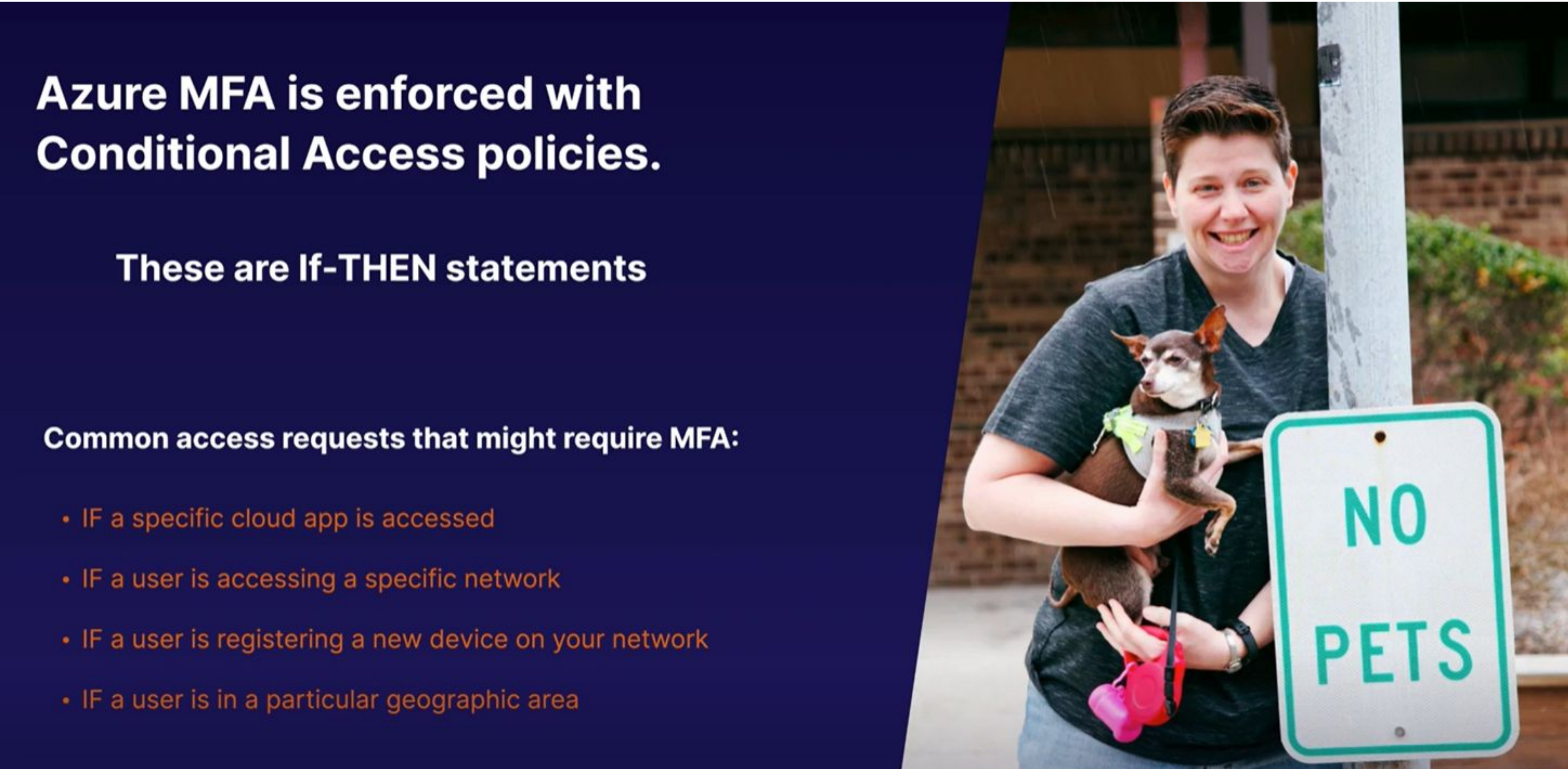
Azure AD Free or standalone O365 licenses

Uses pre-created Conditional Access baseline policies

Azure AD Global Admins

Global Administrator accounts have Azure MFA capabilities built-in

Azure MFA



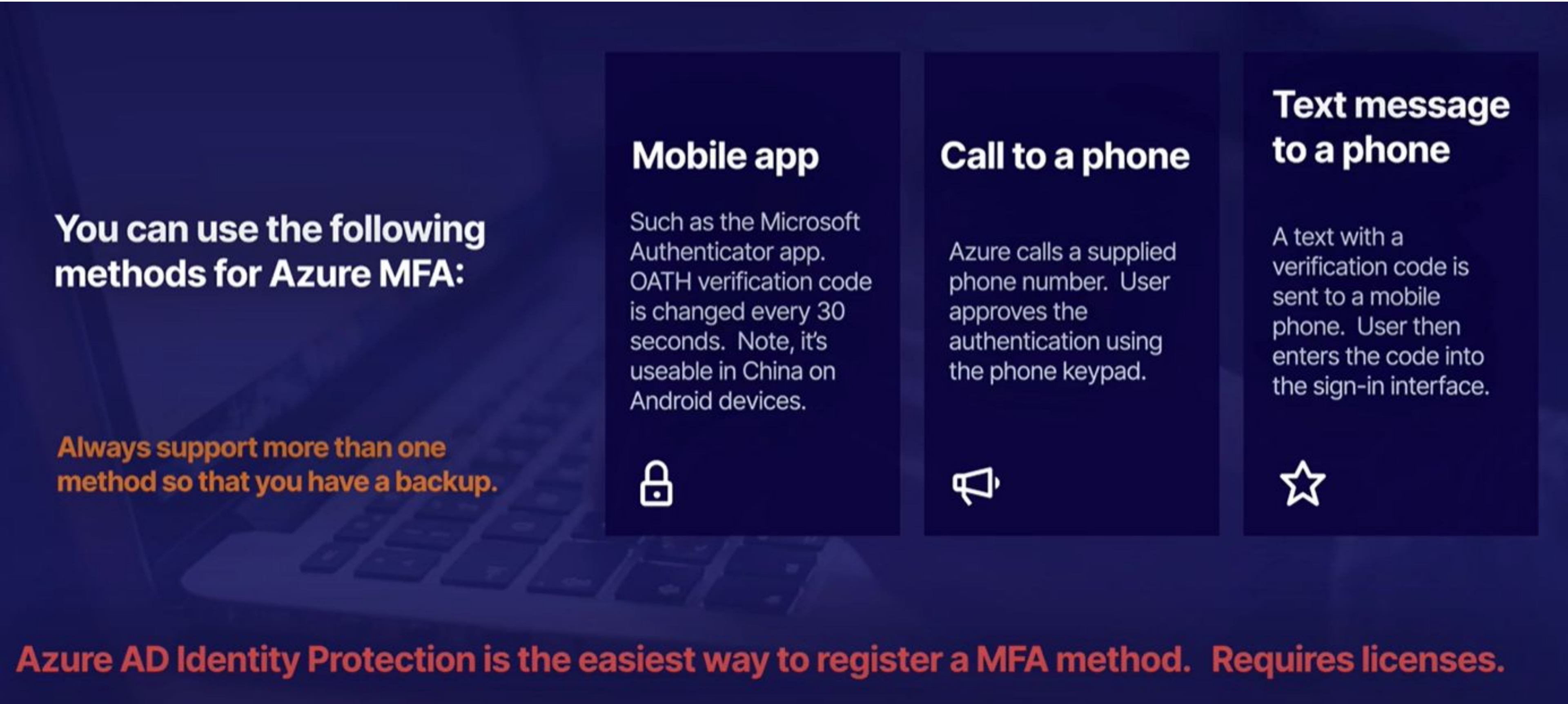
Azure MFA is enforced with Conditional Access policies.

These are If-THEN statements

Common access requests that might require MFA:

- IF a specific cloud app is accessed
- IF a user is accessing a specific network
- IF a user is registering a new device on your network
- IF a user is in a particular geographic area

Supported Authentication Methods



You can use the following methods for Azure MFA:

Always support more than one method so that you have a backup.

Mobile app

Such as the Microsoft Authenticator app. OATH verification code is changed every 30 seconds. Note, it's useable in China on Android devices.

Call to a phone

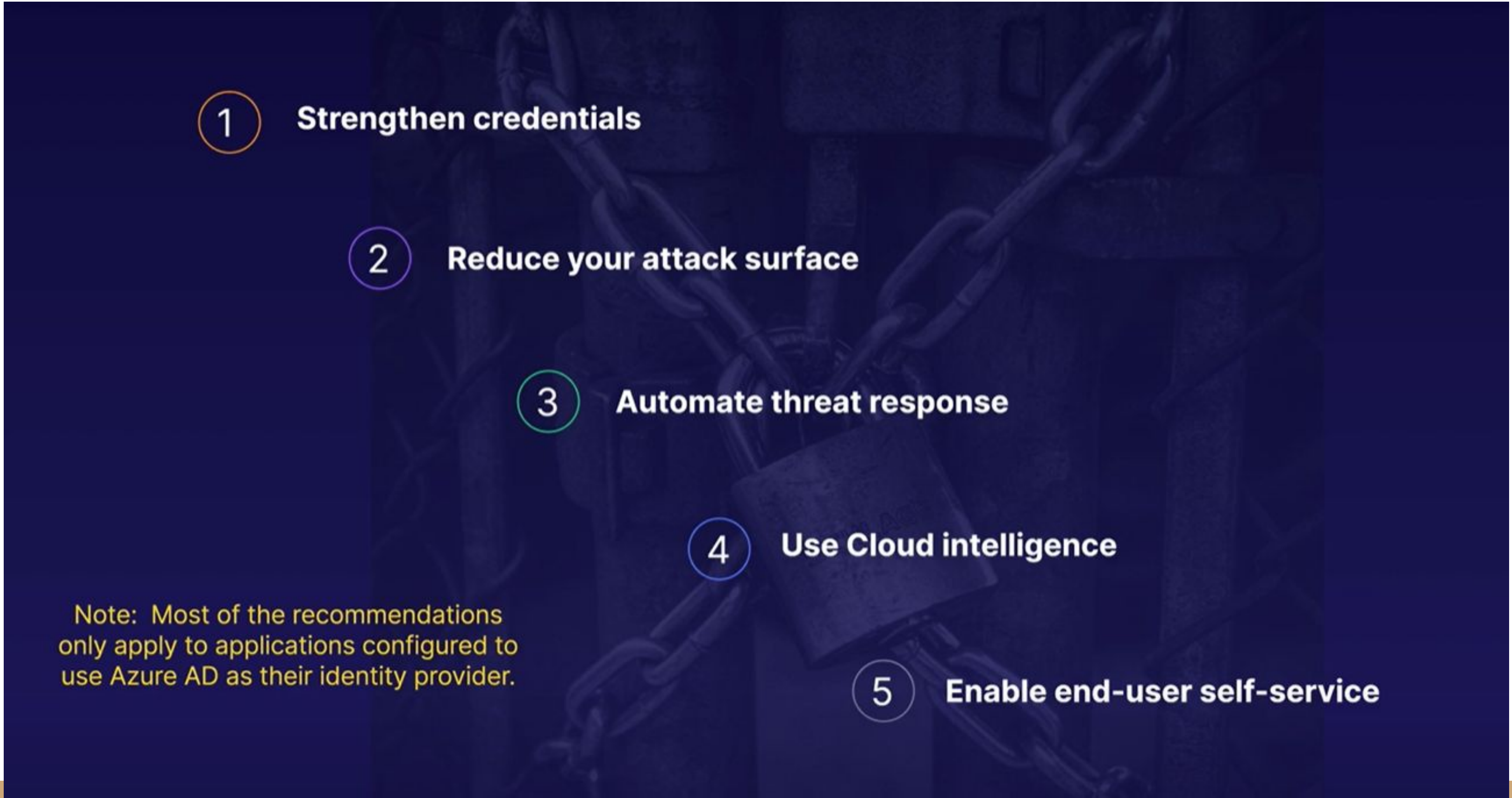
Azure calls a supplied phone number. User approves the authentication using the phone keypad.

Text message to a phone

A text with a verification code is sent to a mobile phone. User then enters the code into the sign-in interface.

Azure AD Identity Protection is the easiest way to register a MFA method. Requires licenses.

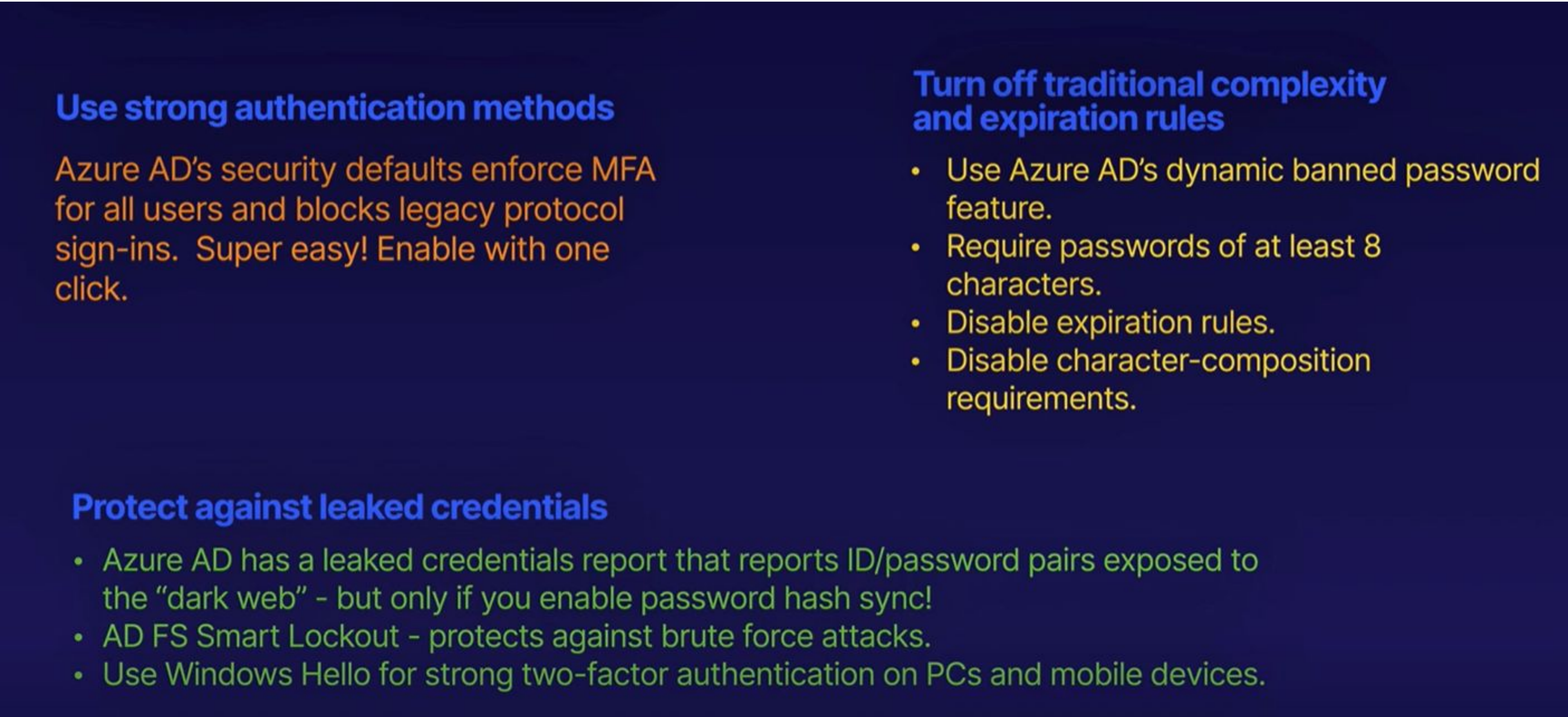
Steps for securing your identity structure



1. Strengthen credentials
2. Reduce your attack surface
3. Automate threat response
4. Use Cloud intelligence
5. Enable end-user self-service

Note: Most of the recommendations only apply to applications configured to use Azure AD as their identity provider.

Strengthen credentials



Use strong authentication methods

Azure AD's security defaults enforce MFA for all users and blocks legacy protocol sign-ins. Super easy! Enable with one click.

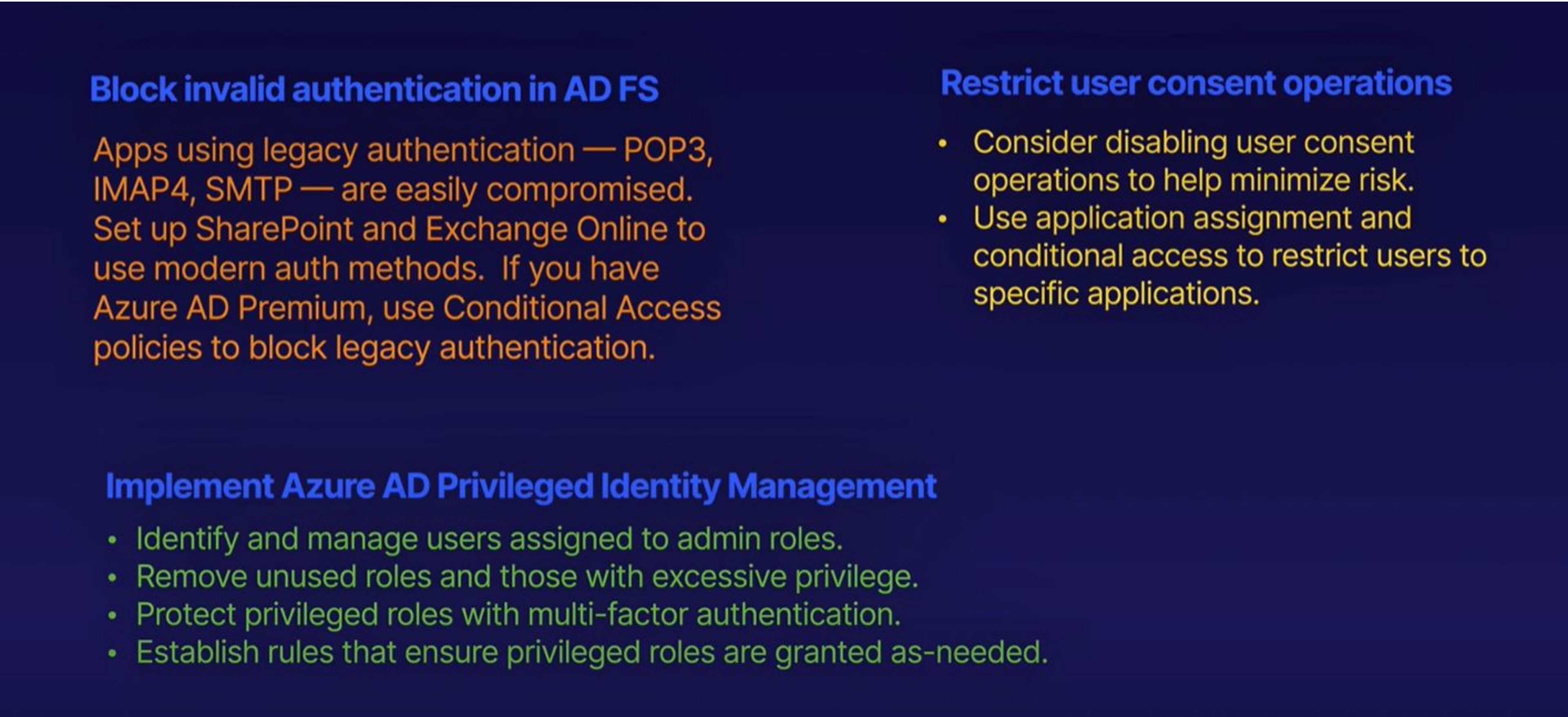
Turn off traditional complexity and expiration rules

- Use Azure AD's dynamic banned password feature.
- Require passwords of at least 8 characters.
- Disable expiration rules.
- Disable character-composition requirements.

Protect against leaked credentials

- Azure AD has a leaked credentials report that reports ID/password pairs exposed to the "dark web" - but only if you enable password hash sync!
- AD FS Smart Lockout - protects against brute force attacks.
- Use Windows Hello for strong two-factor authentication on PCs and mobile devices.

Reduce Attack Surface



Block invalid authentication in AD FS

Apps using legacy authentication — POP3, IMAP4, SMTP — are easily compromised. Set up SharePoint and Exchange Online to use modern auth methods. If you have Azure AD Premium, use Conditional Access policies to block legacy authentication.

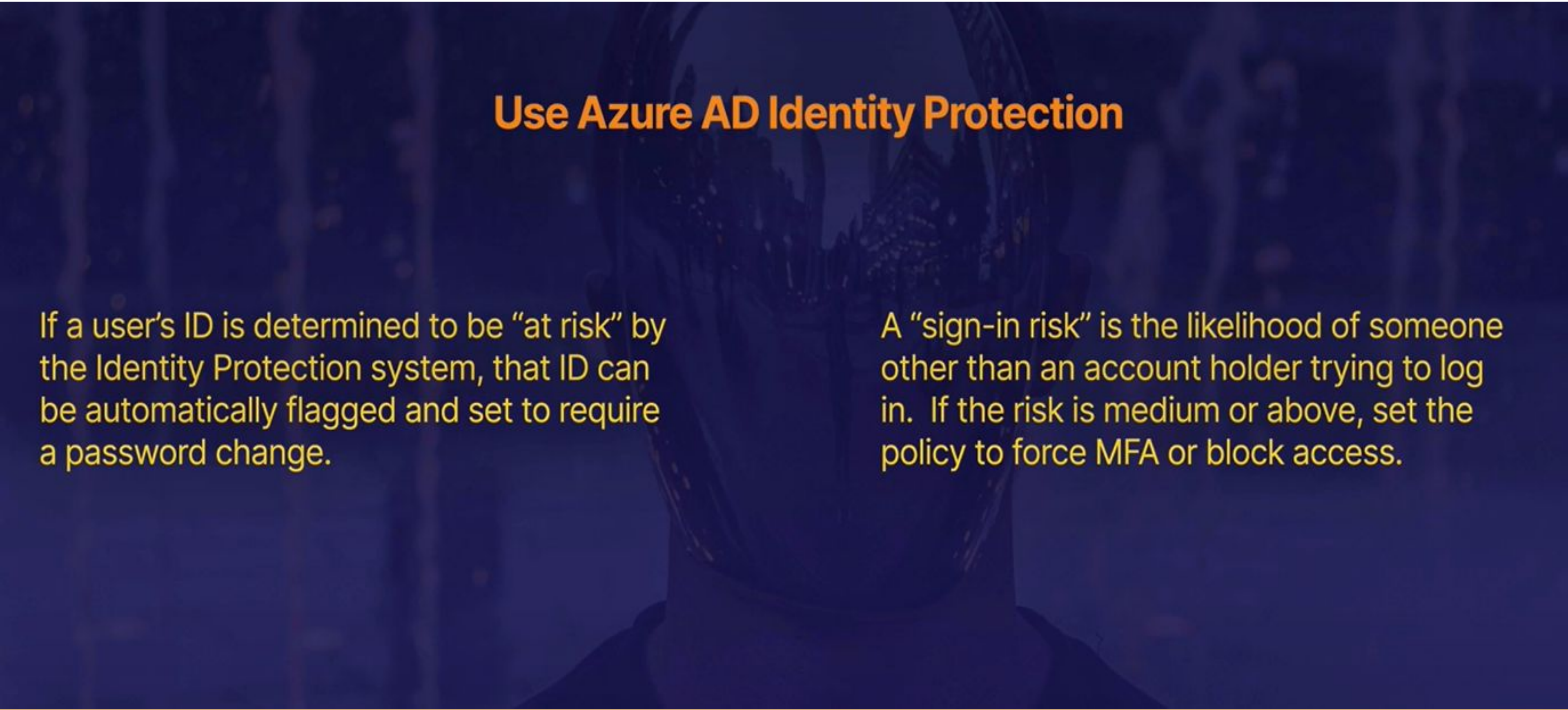
Restrict user consent operations

- Consider disabling user consent operations to help minimize risk.
- Use application assignment and conditional access to restrict users to specific applications.

Implement Azure AD Privileged Identity Management

- Identify and manage users assigned to admin roles.
- Remove unused roles and those with excessive privilege.
- Protect privileged roles with multi-factor authentication.
- Establish rules that ensure privileged roles are granted as-needed.

Automate Threat Response

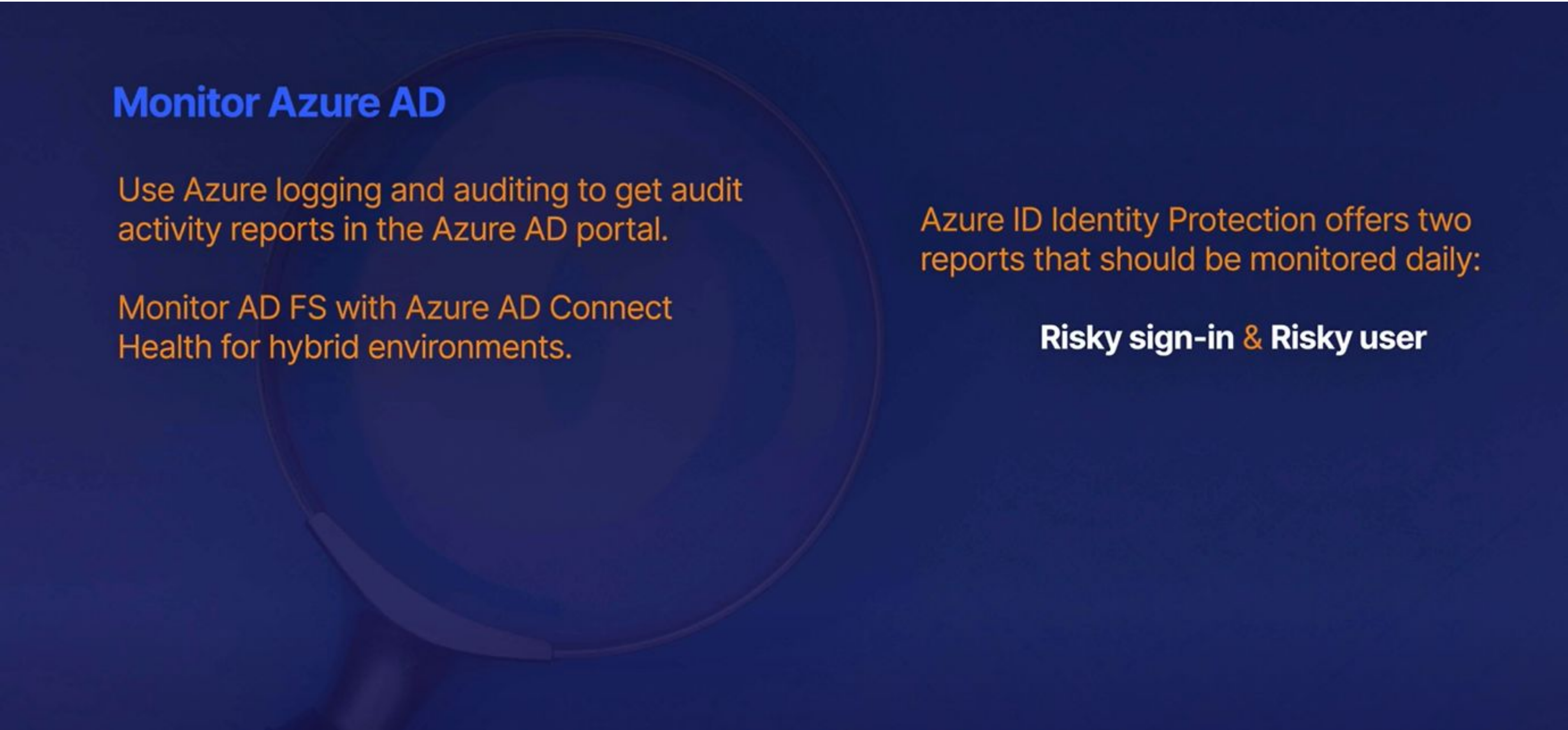


Use Azure AD Identity Protection

If a user's ID is determined to be "at risk" by the Identity Protection system, that ID can be automatically flagged and set to require a password change.

A "sign-in risk" is the likelihood of someone other than an account holder trying to log in. If the risk is medium or above, set the policy to force MFA or block access.

Use Cloud Intelligence



Monitor Azure AD

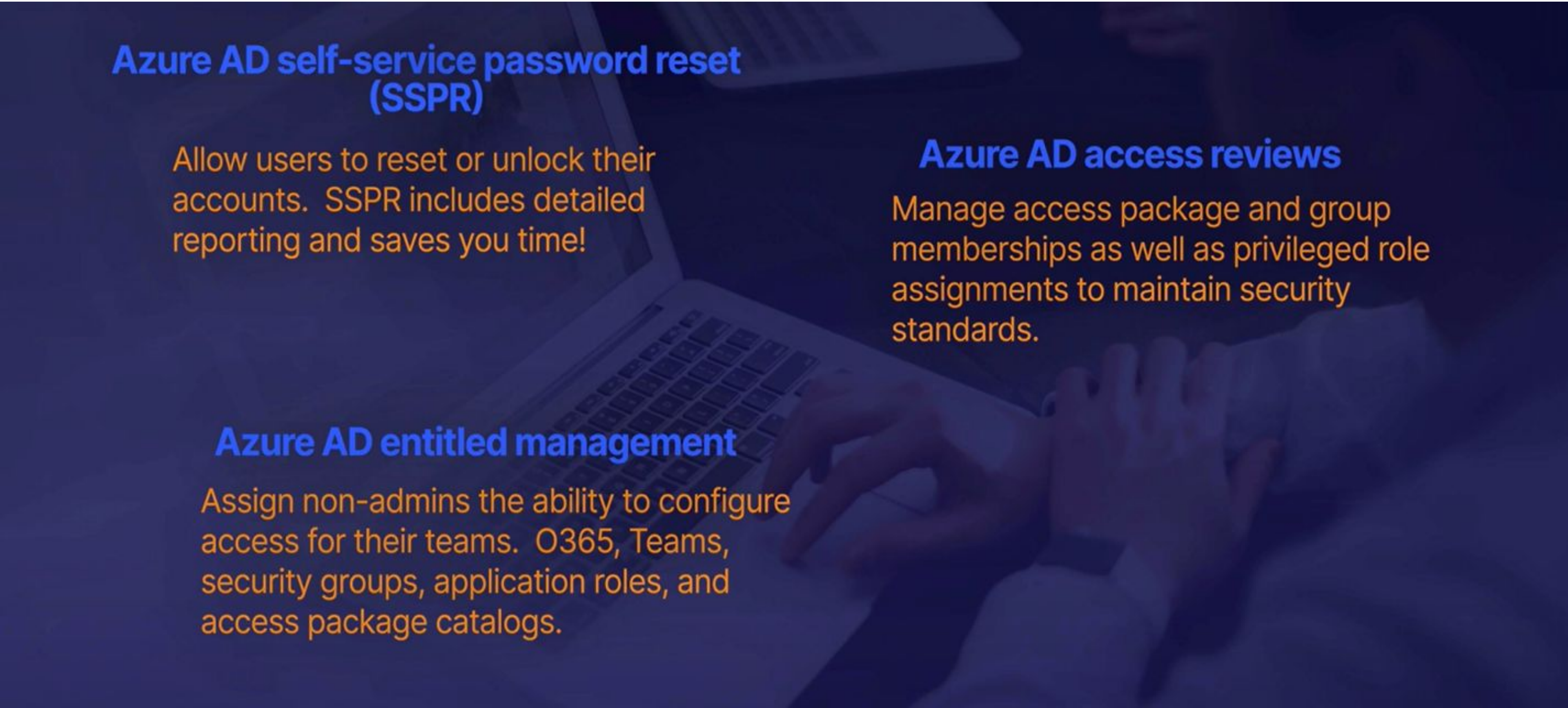
Use Azure logging and auditing to get audit activity reports in the Azure AD portal.

Monitor AD FS with Azure AD Connect Health for hybrid environments.

Azure ID Identity Protection offers two reports that should be monitored daily:

Risky sign-in & **Risky user**

Enable End-User Self-Service



Azure AD self-service password reset (SSPR)

Allow users to reset or unlock their accounts. SSPR includes detailed reporting and saves you time!

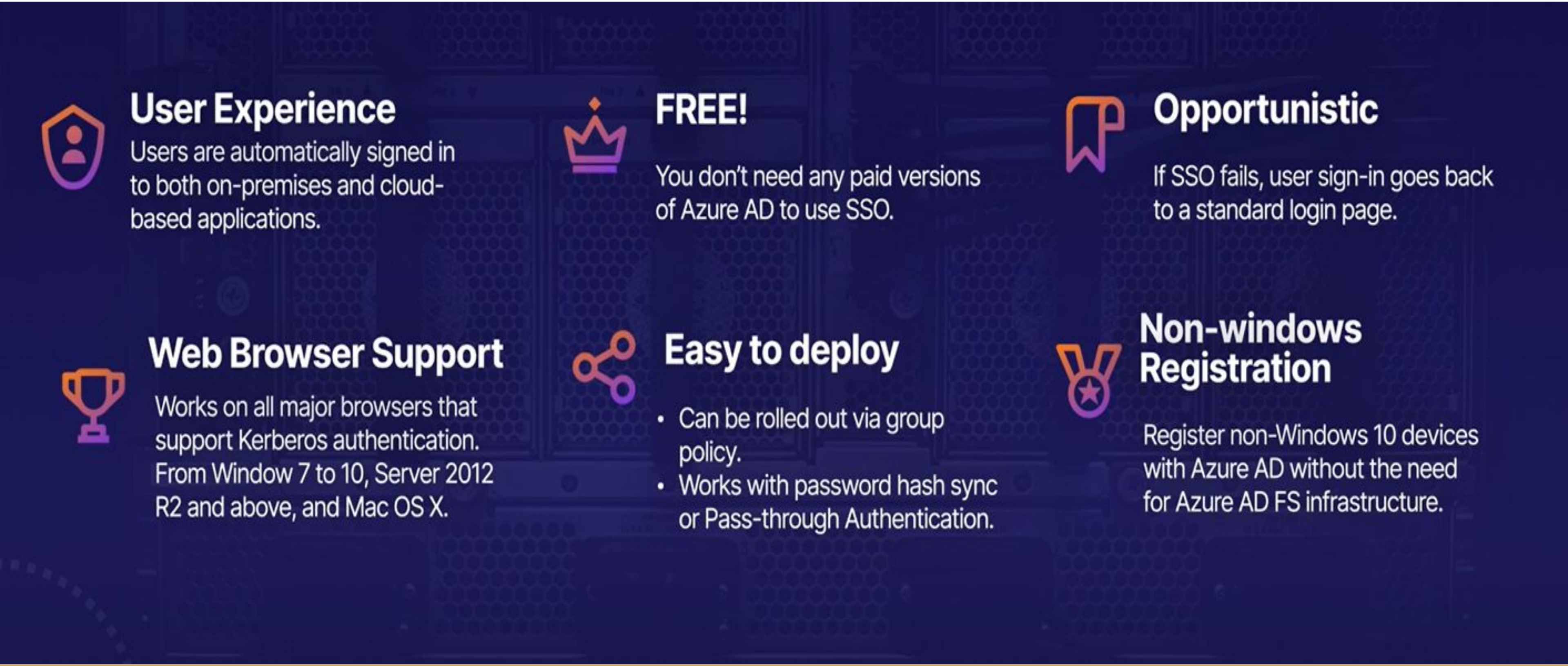
Azure AD access reviews

Manage access package and group memberships as well as privileged role assignments to maintain security standards.

Azure AD entitled management

Assign non-admins the ability to configure access for their teams. O365, Teams, security groups, application roles, and access package catalogs.

Key Features of Azure Seamless Single Sign-On



User Experience

Users are automatically signed in to both on-premises and cloud-based applications.

FREE!

You don't need any paid versions of Azure AD to use SSO.

Opportunistic

If SSO fails, user sign-in goes back to a standard login page.

Web Browser Support

Works on all major browsers that support Kerberos authentication. From Window 7 to 10, Server 2012 R2 and above, and Mac OS X.

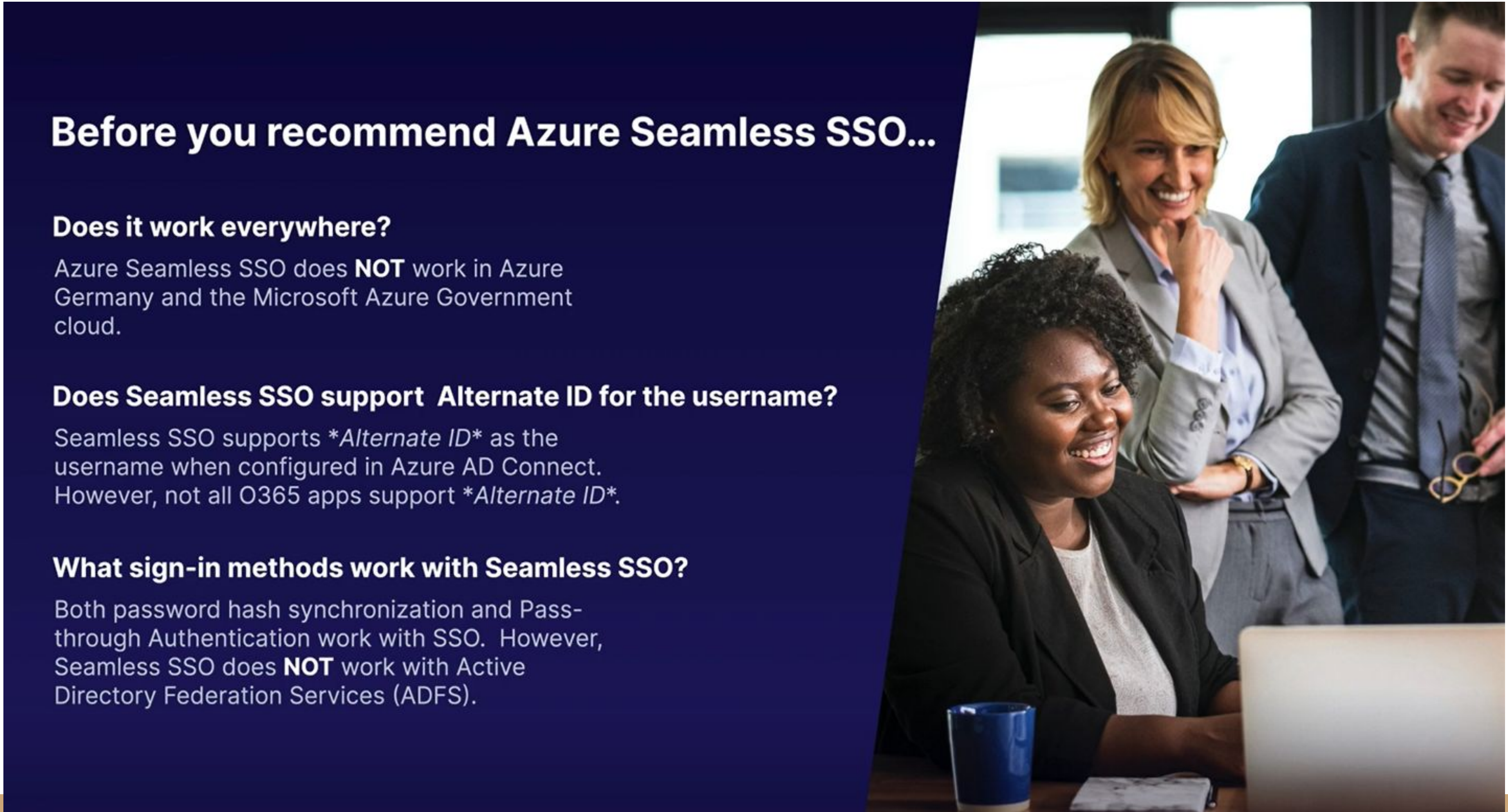
Easy to deploy

- Can be rolled out via group policy.
- Works with password hash sync or Pass-through Authentication.

Non-windows Registration

Register non-Windows 10 devices with Azure AD without the need for Azure AD FS infrastructure.

Azure Seamless Single Sign-On



Before you recommend Azure Seamless SSO...

Does it work everywhere?

Azure Seamless SSO does **NOT** work in Azure Germany and the Microsoft Azure Government cloud.

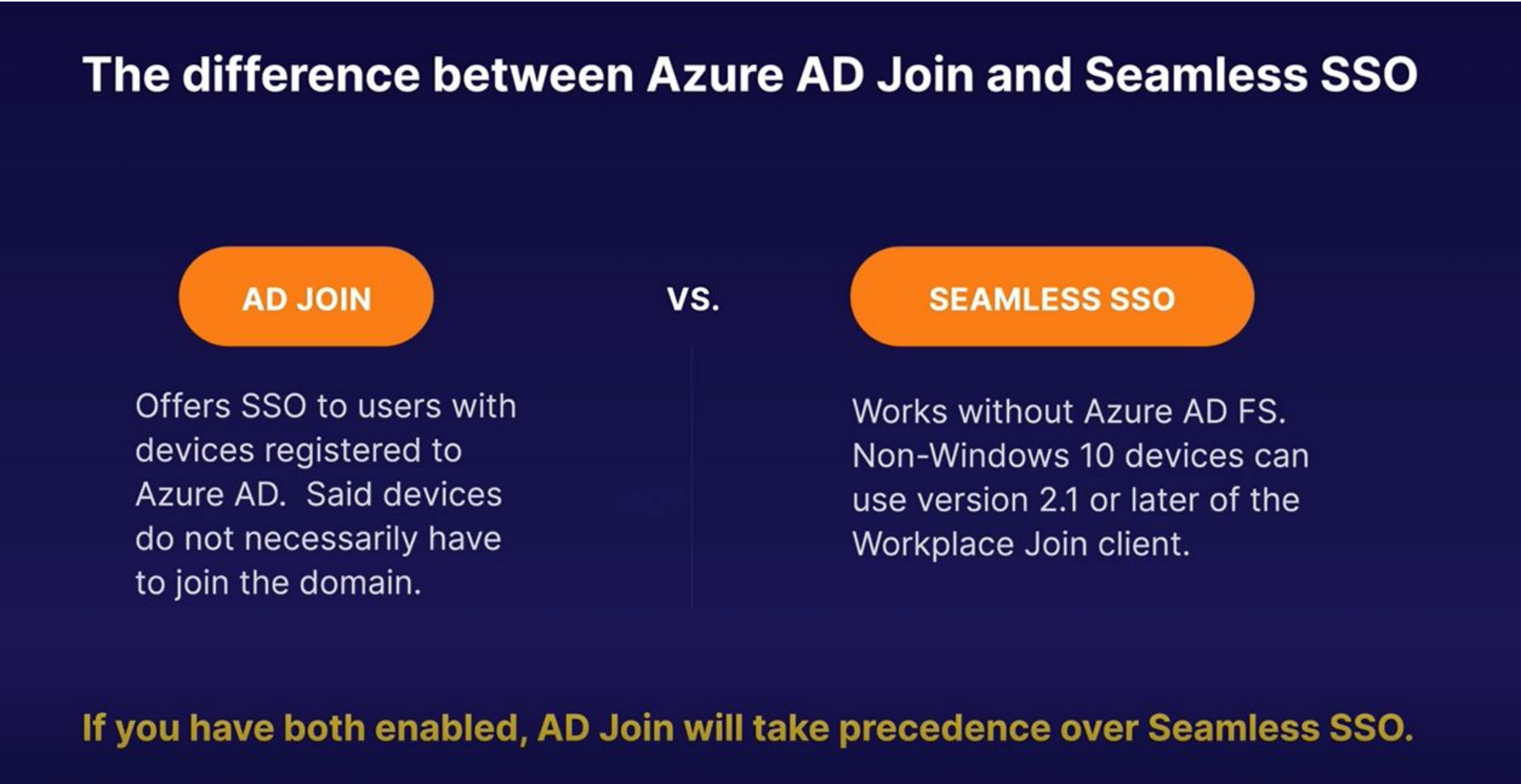
Does Seamless SSO support Alternate ID for the username?

Seamless SSO supports *Alternate ID* as the username when configured in Azure AD Connect. However, not all O365 apps support *Alternate ID*.

What sign-in methods work with Seamless SSO?

Both password hash synchronization and Pass-through Authentication work with SSO. However, Seamless SSO does **NOT** work with Active Directory Federation Services (ADFS).

AD Join vs Sleamless SSO



The difference between Azure AD Join and Seamless SSO

AD JOIN vs. **SEAMLESS SSO**

AD JOIN

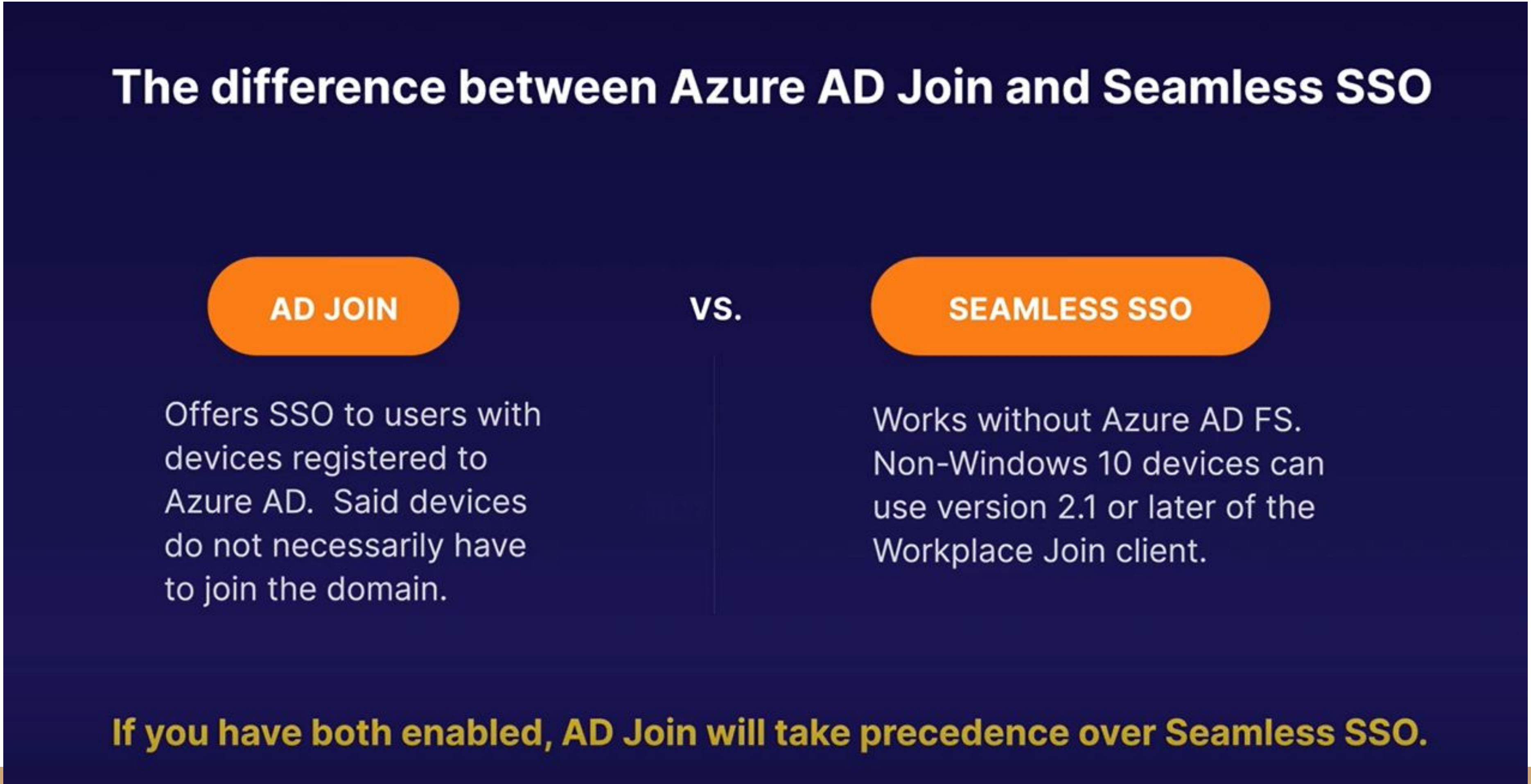
Offers SSO to users with devices registered to Azure AD. Said devices do not necessarily have to join the domain.

SEAMLESS SSO

Works without Azure AD FS. Non-Windows 10 devices can use version 2.1 or later of the Workplace Join client.

If you have both enabled, AD Join will take precedence over Seamless SSO.

The difference between Azure AD Join and Seamless SSO



The difference between Azure AD Join and Seamless SSO

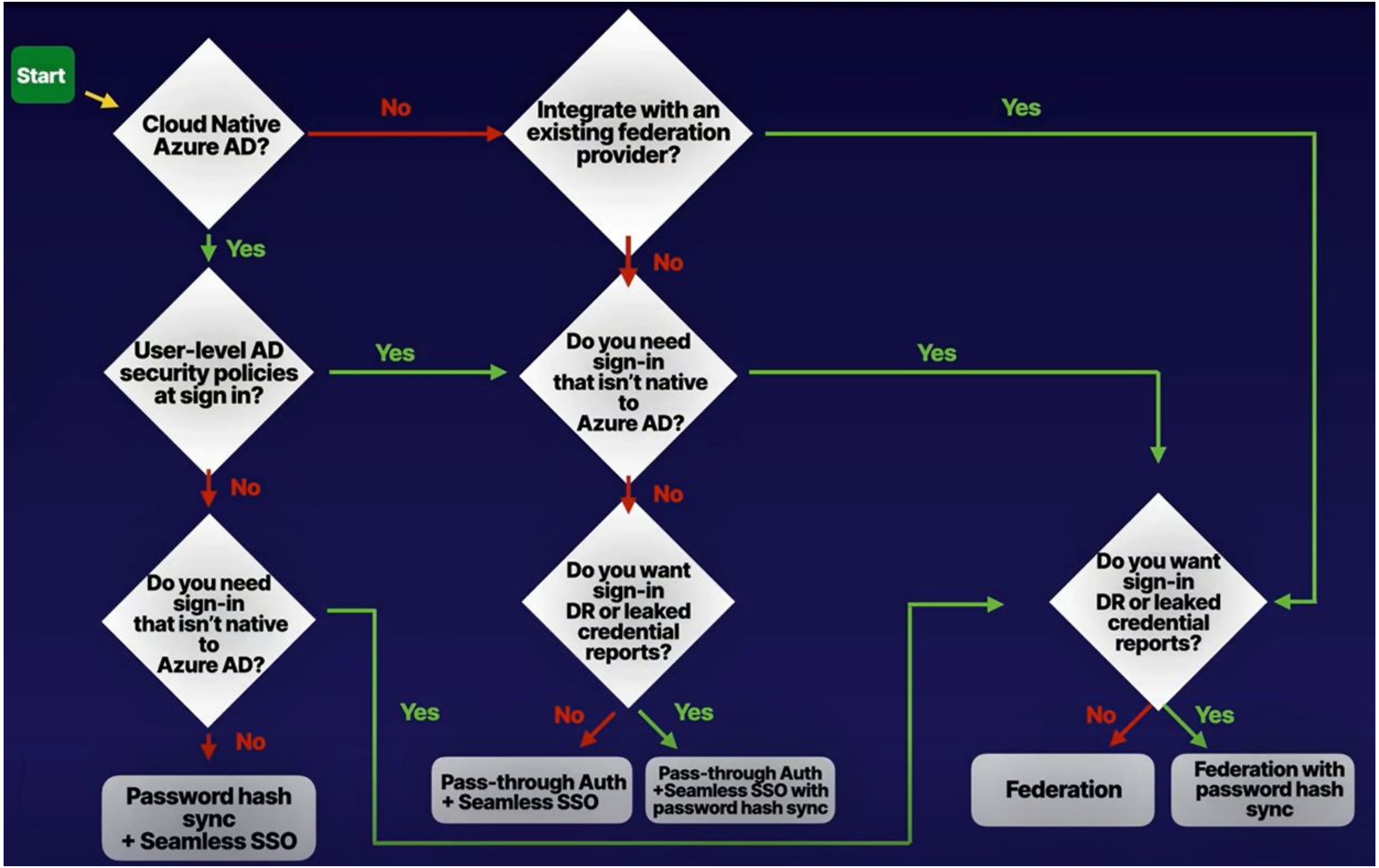
AD JOIN vs. **SEAMLESS SSO**

Offers SSO to users with devices registered to Azure AD. Said devices do not necessarily have to join the domain.

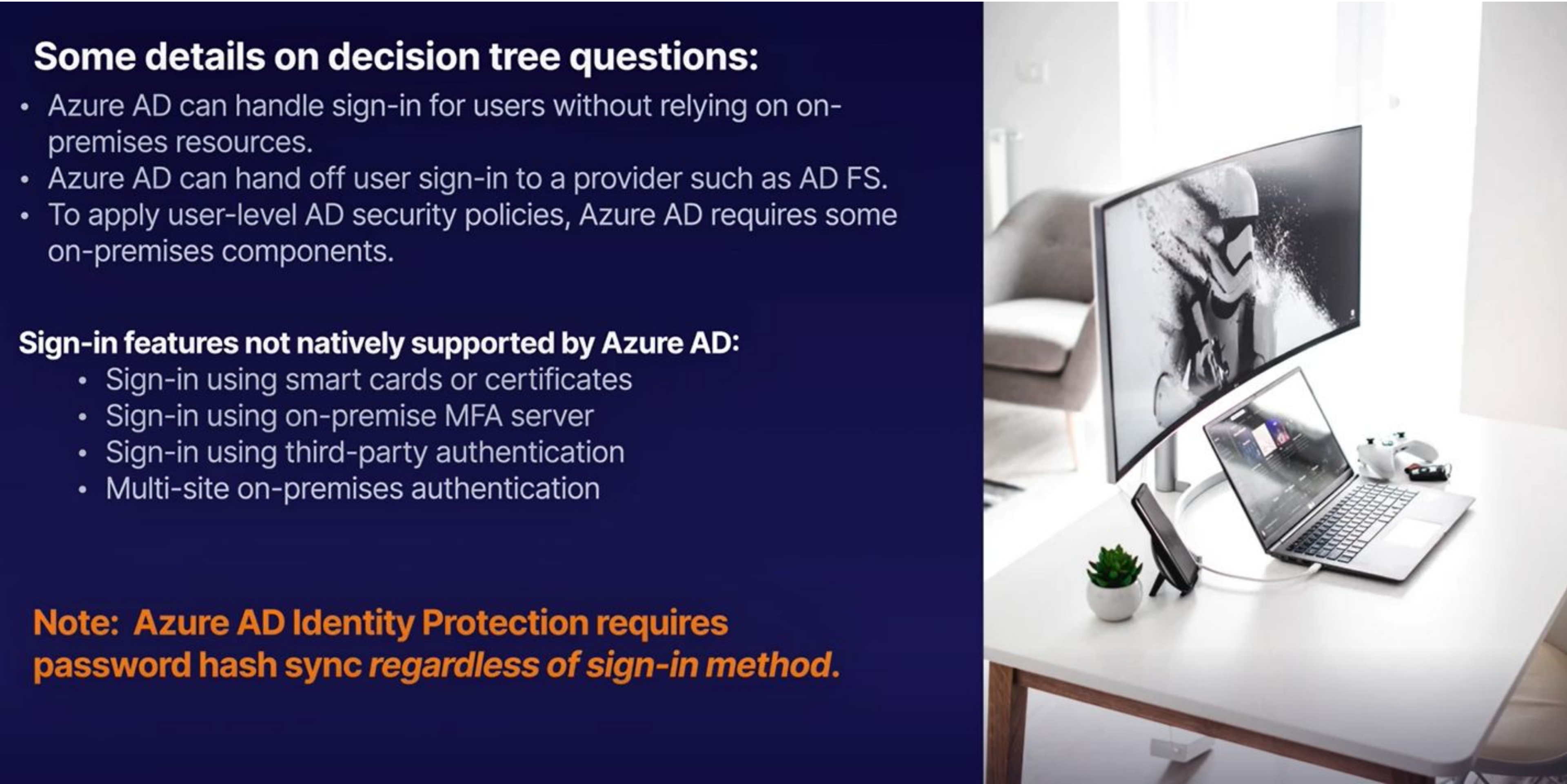
Works without Azure AD FS. Non-Windows 10 devices can use version 2.1 or later of the Workplace Join client.

If you have both enabled, AD Join will take precedence over Seamless SSO.

Hybrid Identity Decision Tree


Start
Cloud Native Azure AD?
No
Integrate with an existing federation provider?
Yes
Yes
No
User-level AD security policies at sign in?
Yes
Do you need sign-in that isn't native to Azure AD?
Yes
No
No
Do you need sign-in that isn't native to Azure AD?
Do you want sign-in DR or leaked credential reports?
Do you want sign-in DR or leaked credential reports?
Yes
No
No
Yes
No
Yes
Password hash sync + Seamless SSO
Pass-through Auth + Seamless SSO
Pass-through Auth +Seamless SSO with password hash sync
Federation
Federation with password hash sync

Hybrid Identity Decision Tree



Some details on decision tree questions:

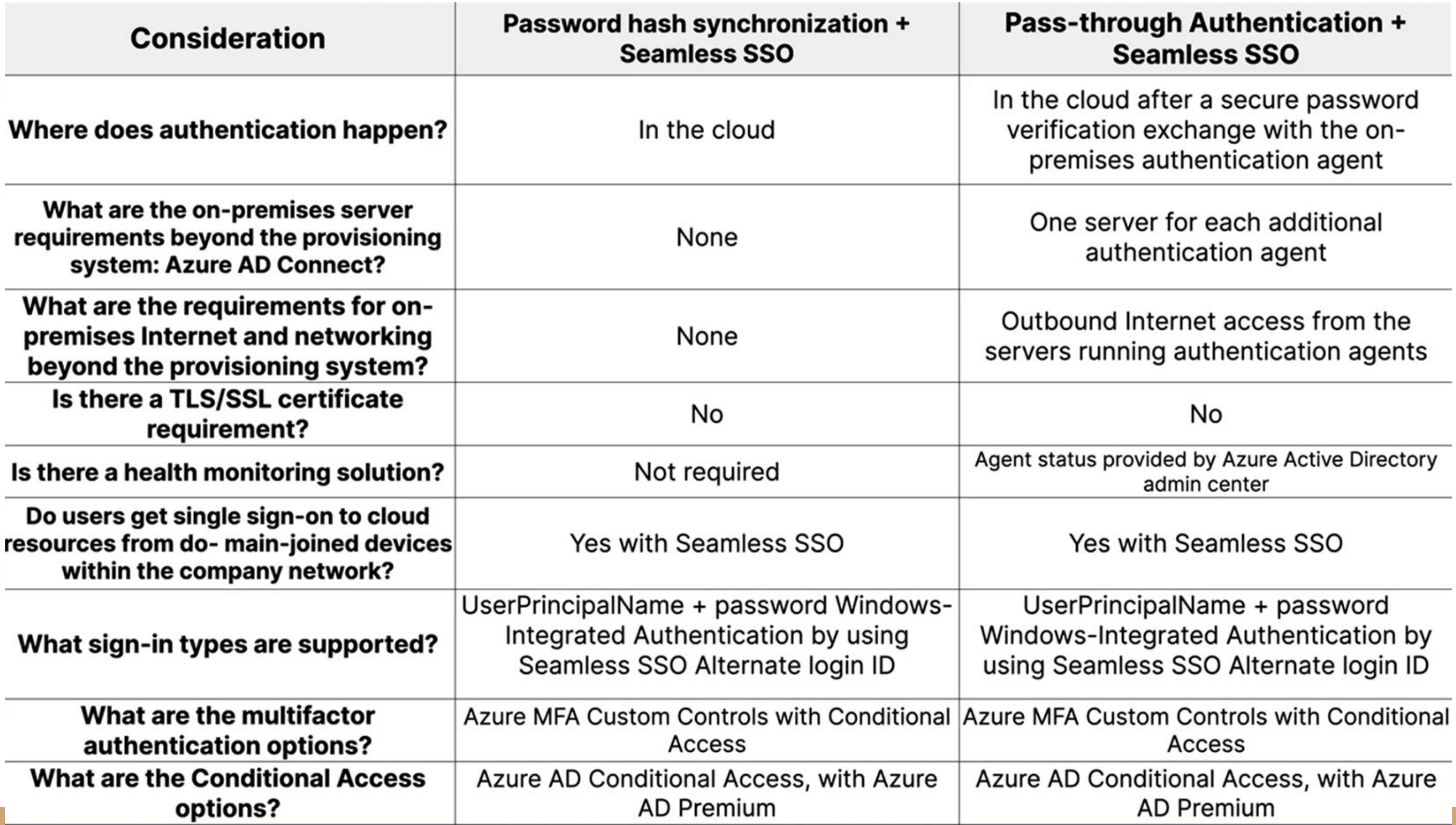
- Azure AD can handle sign-in for users without relying on on-premises resources.
- Azure AD can hand off user sign-in to a provider such as AD FS.
- To apply user-level AD security policies, Azure AD requires some on-premises components.

Sign-in features not natively supported by Azure AD:

- Sign-in using smart cards or certificates
- Sign-in using on-premise MFA server
- Sign-in using third-party authentication
- Multi-site on-premises authentication

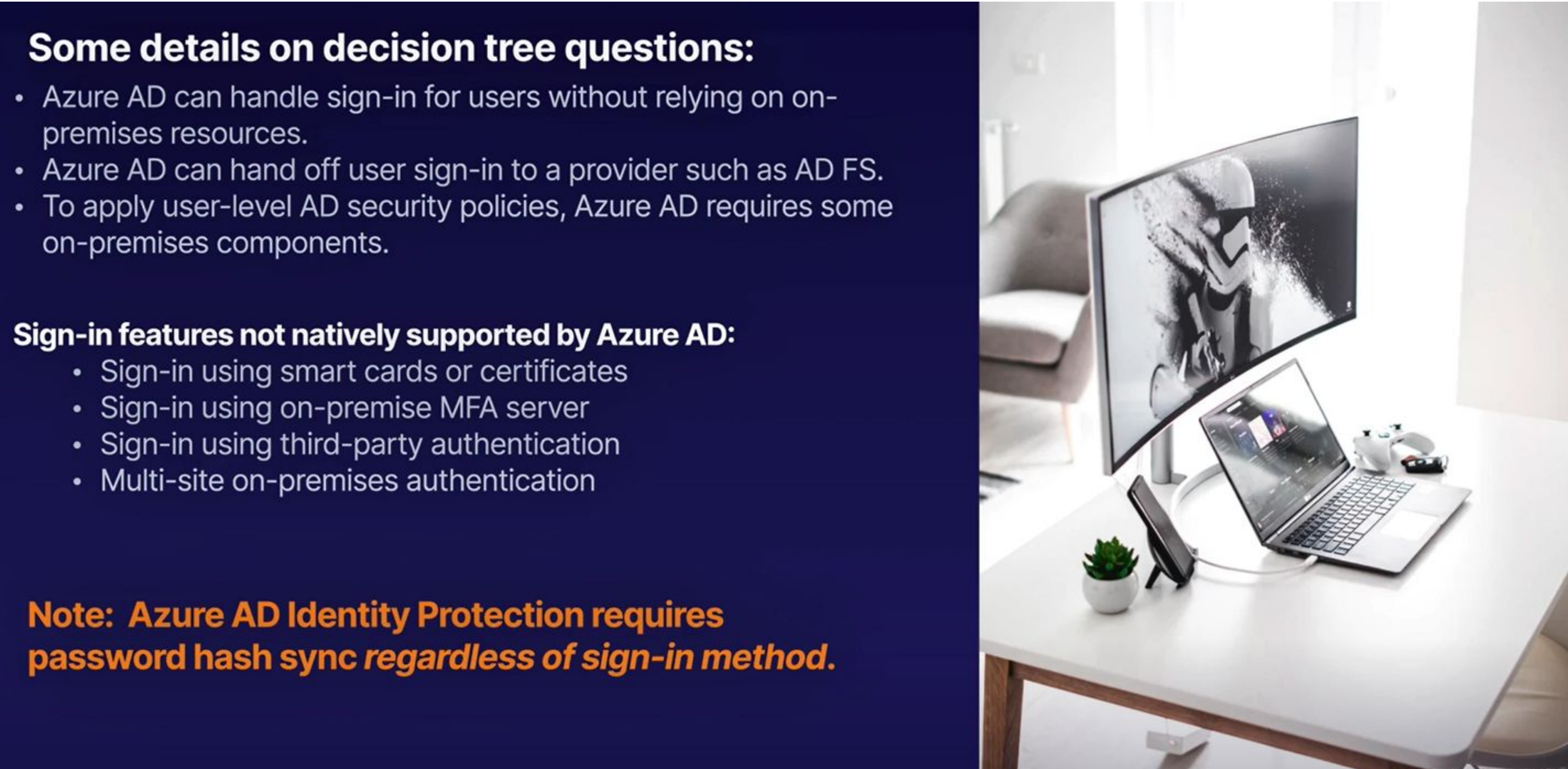
Note: Azure AD Identity Protection requires password hash sync *regardless of sign-in method.*

Hybrid Identity Decision Tree



Consideration	Password hash synchronization + Seamless SSO	Pass-through Authentication + Seamless SSO
Where does authentication happen?	In the cloud	In the cloud after a secure password verification exchange with the on-premises authentication agent
What are the on-premises server requirements beyond the provisioning system: Azure AD Connect?	None	One server for each additional authentication agent
What are the requirements for on-premises Internet and networking beyond the provisioning system?	None	Outbound Internet access from the servers running authentication agents
Is there a TLS/SSL certificate requirement?	No	No
Is there a health monitoring solution?	Not required	Agent status provided by Azure Active Directory admin center
Do users get single sign-on to cloud resources from do- main-joined devices within the company network?	Yes with Seamless SSO	Yes with Seamless SSO
What sign-in types are supported?	UserPrincipalName + password Windows-Integrated Authentication by using Seamless SSO Alternate login ID	UserPrincipalName + password Windows-Integrated Authentication by using Seamless SSO Alternate login ID
What are the multifactor authentication options?	Azure MFA Custom Controls with Conditional Access	Azure MFA Custom Controls with Conditional Access
What are the Conditional Access options?	Azure AD Conditional Access, with Azure AD Premium	Azure AD Conditional Access, with Azure AD Premium

Hybrid Identity Decision Tree



Some details on decision tree questions:

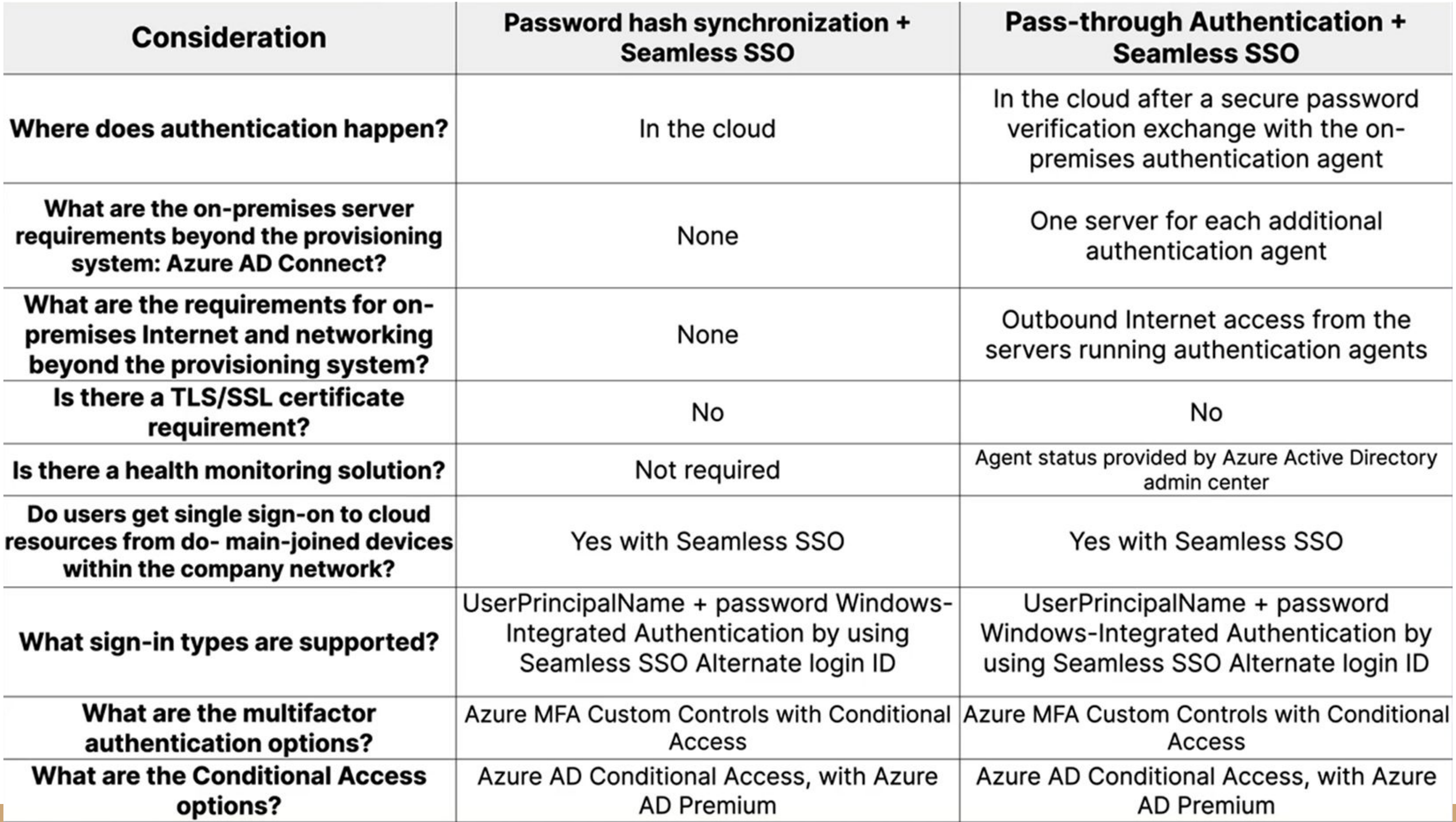
- Azure AD can handle sign-in for users without relying on on-premises resources.
- Azure AD can hand off user sign-in to a provider such as AD FS.
- To apply user-level AD security policies, Azure AD requires some on-premises components.

Sign-in features not natively supported by Azure AD:

- Sign-in using smart cards or certificates
- Sign-in using on-premise MFA server
- Sign-in using third-party authentication
- Multi-site on-premises authentication

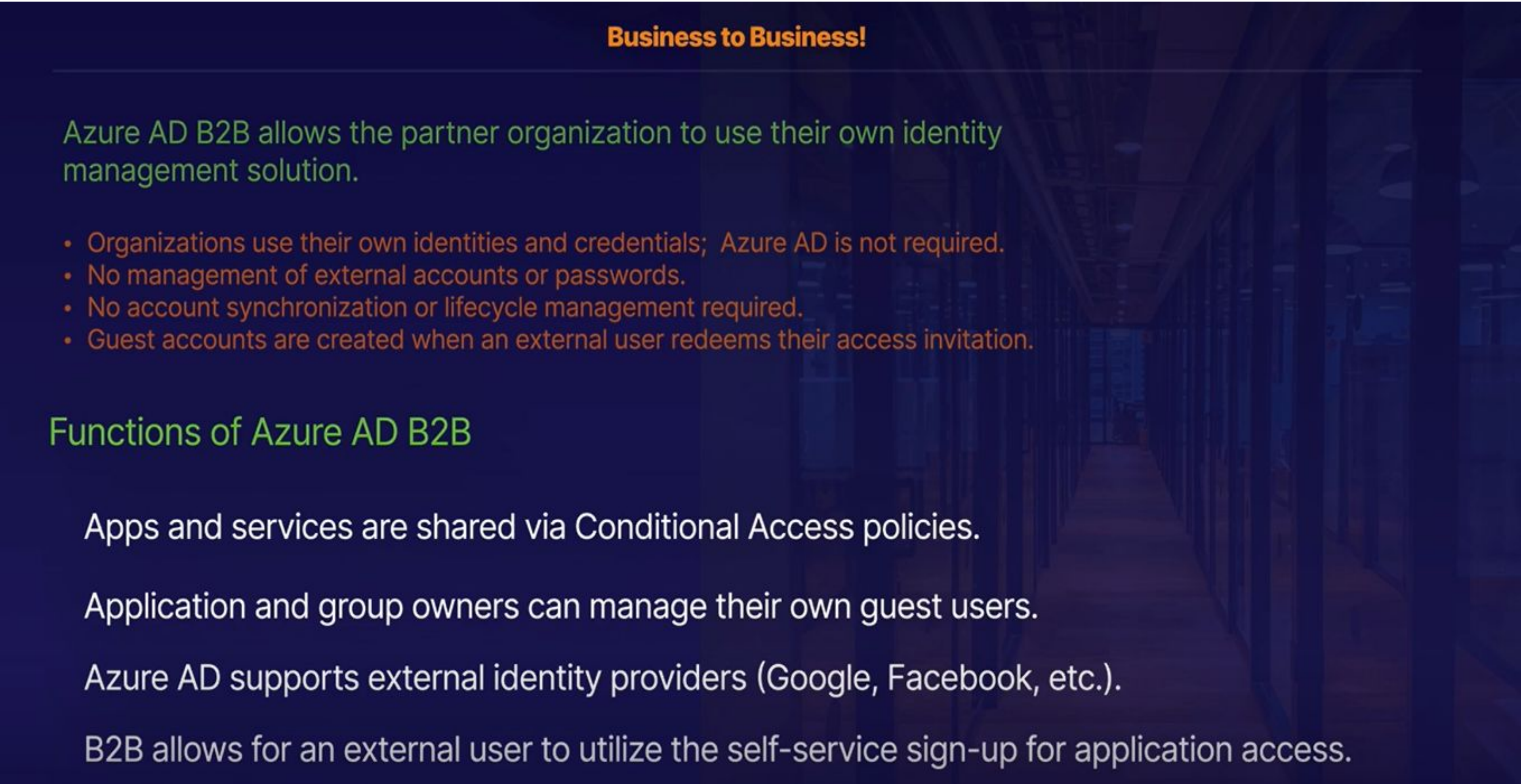
Note: Azure AD Identity Protection requires password hash sync *regardless of sign-in method*.

Comparing Authentication Methods



Consideration	Password hash synchronization + Seamless SSO	Pass-through Authentication + Seamless SSO
Where does authentication happen?	In the cloud	In the cloud after a secure password verification exchange with the on-premises authentication agent
What are the on-premises server requirements beyond the provisioning system: Azure AD Connect?	None	One server for each additional authentication agent
What are the requirements for on-premises Internet and networking beyond the provisioning system?	None	Outbound Internet access from the servers running authentication agents
Is there a TLS/SSL certificate requirement?	No	No
Is there a health monitoring solution?	Not required	Agent status provided by Azure Active Directory admin center
Do users get single sign-on to cloud resources from do- main-joined devices within the company network?	Yes with Seamless SSO	Yes with Seamless SSO
What sign-in types are supported?	UserPrincipalName + password Windows-Integrated Authentication by using Seamless SSO Alternate login ID	UserPrincipalName + password Windows-Integrated Authentication by using Seamless SSO Alternate login ID
What are the multifactor authentication options?	Azure MFA Custom Controls with Conditional Access	Azure MFA Custom Controls with Conditional Access
What are the Conditional Access options?	Azure AD Conditional Access, with Azure AD Premium	Azure AD Conditional Access, with Azure AD Premium

B2B - What Is It?



Business to Business!

Azure AD B2B allows the partner organization to use their own identity management solution.

- Organizations use their own identities and credentials; Azure AD is not required.
- No management of external accounts or passwords.
- No account synchronization or lifecycle management required.
- Guest accounts are created when an external user redeems their access invitation.

Functions of Azure AD B2B

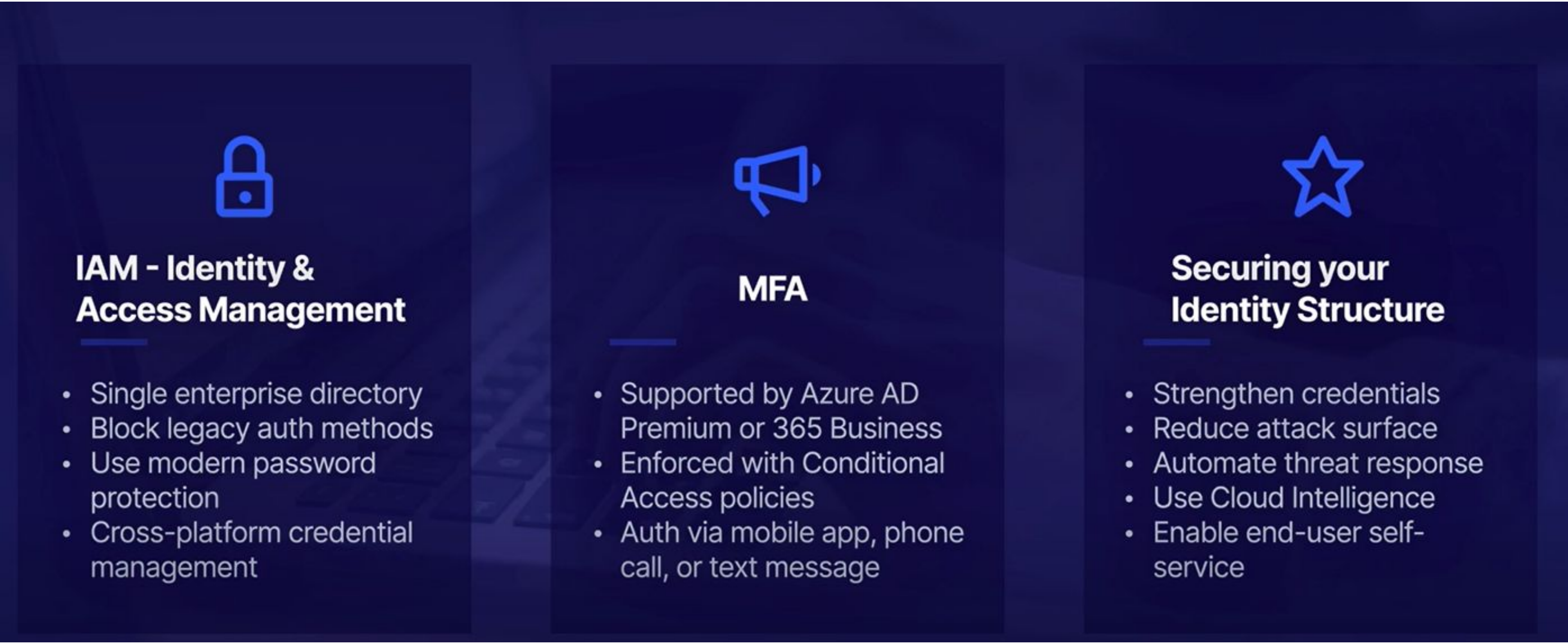
Apps and services are shared via Conditional Access policies.

Application and group owners can manage their own guest users.

Azure AD supports external identity providers (Google, Facebook, etc.).

B2B allows for an external user to utilize the self-service sign-up for application access.

Summary



IAM - Identity & Access Management

- Single enterprise directory
- Block legacy auth methods
- Use modern password protection
- Cross-platform credential management

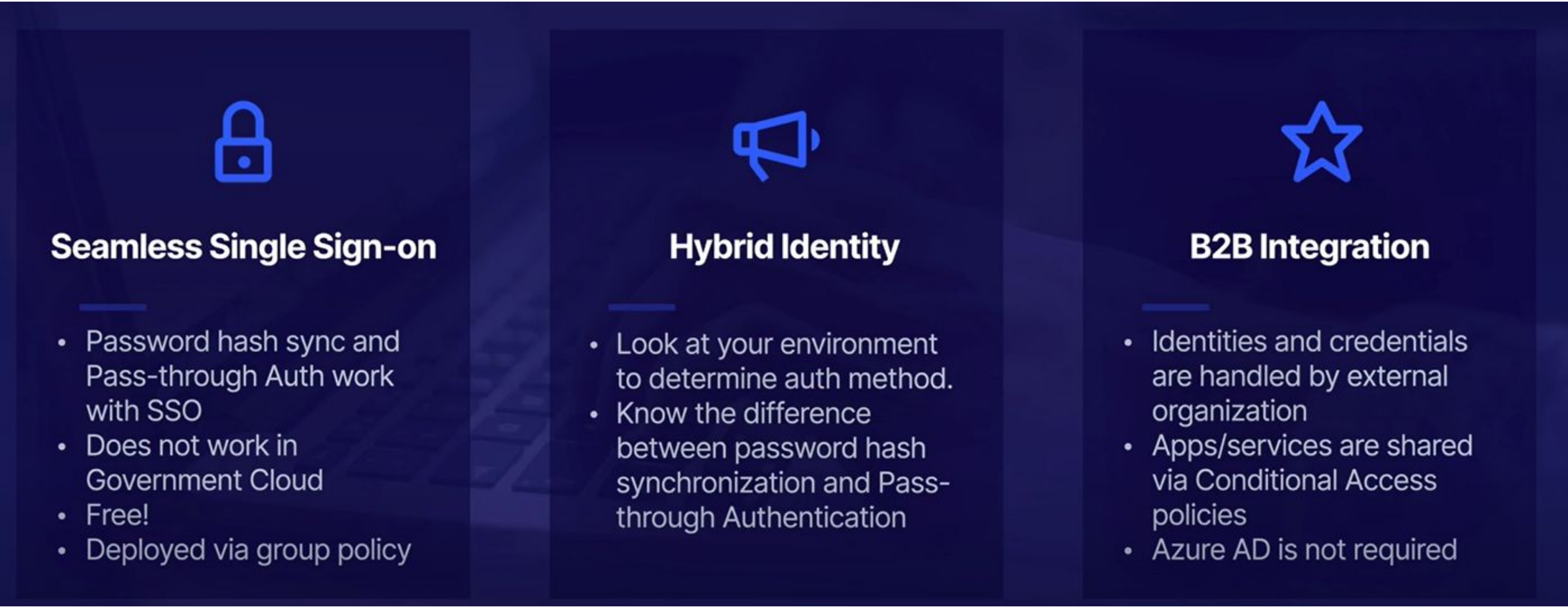
MFA

- Supported by Azure AD Premium or 365 Business
- Enforced with Conditional Access policies
- Auth via mobile app, phone call, or text message

Securing your Identity Structure

- Strengthen credentials
- Reduce attack surface
- Automate threat response
- Use Cloud Intelligence
- Enable end-user self-service

Summary



Seamless Single Sign-on

- Password hash sync and Pass-through Auth work with SSO
- Does not work in Government Cloud
- Free!
- Deployed via group policy

Hybrid Identity

- Look at your environment to determine auth method.
- Know the difference between password hash synchronization and Pass-through Authentication

B2B Integration

- Identities and credentials are handled by external organization
- Apps/services are shared via Conditional Access policies
- Azure AD is not required

Thank you!