ICT POWER.IT

Microsoft MVP Microsoft® Most Valuable Professional

Microsoft

#POWERCON2020

Azure Active Directory come Security Boundary

Nicola Ferrini

Microsoft Most Valuable Professional

Cloud and Datacenter Management

/NicolaFerrini.it

@nicolaferrini

Who Am I ?

Microsoft Certified Trainer — Microsoft MCT Trainer — 2020 - 2021

ICT POWER.IT

Microsoft Certified Professional — Microsoft MCSE Productivity — Earned 2016

Microsoft Certified Professional — Microsoft MCSE Cloud Platform and Infrastructure — Earned 2016

Microsoft Regional Director

MVP Microsoft® Most Valuable Professional

VeeAM Certified Engineer 2020

vmware 2X Certified Professional DCV & Desktop Mobility — Milestone

aws certified Cloud Practitioner

aws certified Solutions Architect Associate

Microsoft Certified Azure Security Engineer Associate

Microsoft 365 Certified Messaging Administrator Associate

Microsoft 365 Certified Security Administrator Associate

Microsoft 365 Certified Modern Desktop Administrator Associate

Microsoft Certified Azure Solutions Architect Expert

Microsoft 365 Certified Enterprise Administrator Expert

Identity and access become the new primary security boundary

- Network perimeters, firewalls, and physical access controls used to be the primary protection for corporate data. But network perimeters have become increasingly porous with the explosion of bring your own device (BYOD), mobile apps, cloud applications and **pandemic**.

- Identity has become the new primary security boundary. Therefore, proper authentication and assignment of privileges is critical to maintaining control of your data.

- Two fundamental concepts that need to be understood when talking about identity and access control are **authentication** (sometimes shortened to *AuthN*) and **authorization** (sometimes shortened to *AuthZ*).

Secure remote workers

It can seem daunting trying to secure your workers in today's world, especially when you must respond rapidly and provide access to many services quickly.

Azure AD offers many features and provides many layers of security for your Identities:

- Strengthen your credentials.
- Reduce your attack surface area.
- Automate threat response.
- Utilize cloud intelligence.
- Enable end-user self-service.

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-secure-remote-workers

Microsoft Azure Active Directory again a “Leader” in Gartner Magic Quadrant for Access Management

Figure 1: Magic Quadrant for Access Management

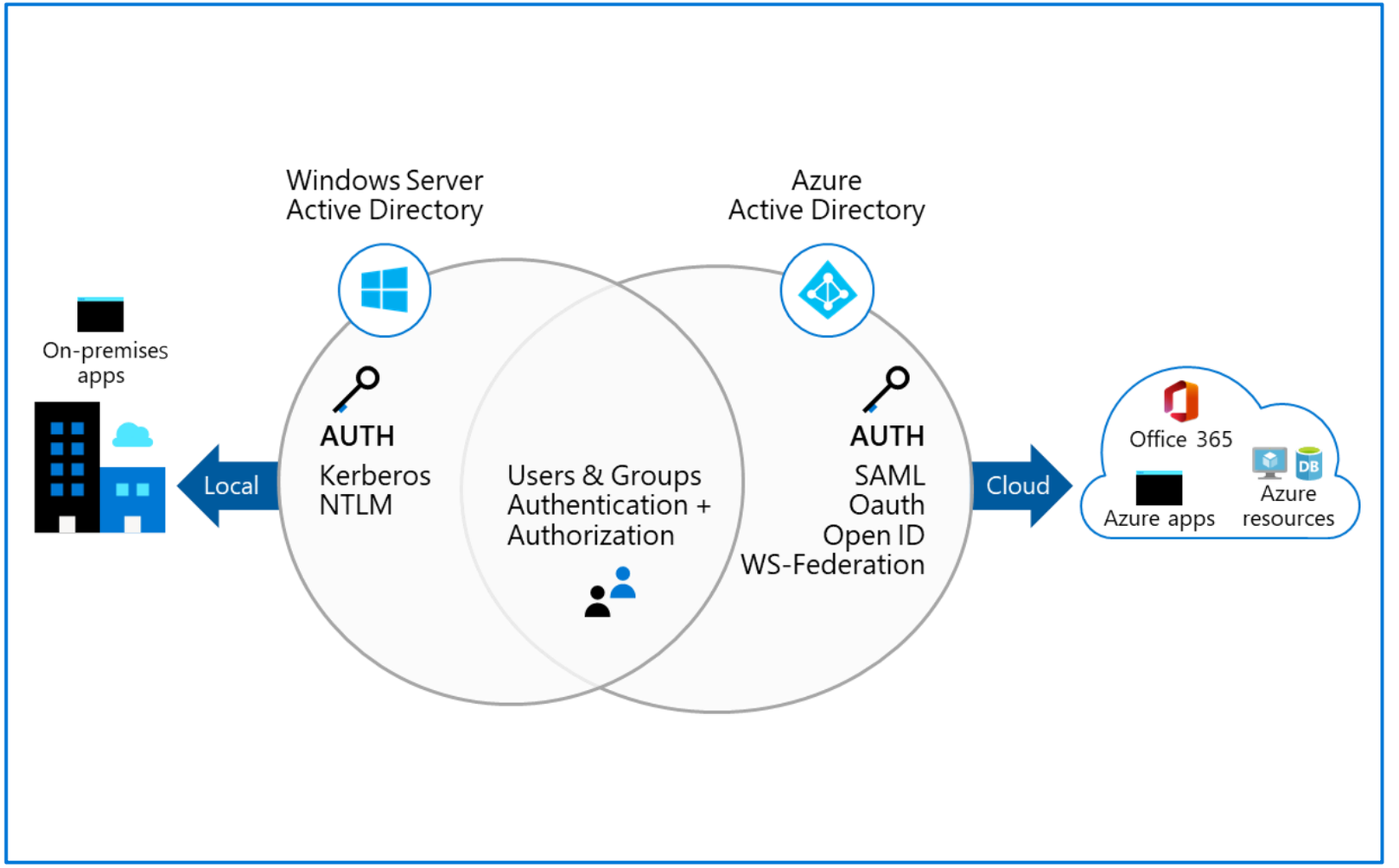
Source: Gartner (November 2020)

https://www.microsoft.com/security/blog/2020/11/24/microsoft-azure-active-directory-again-a-leader-in-gartner-magic-quadrant-for-access-management/

Azure Active Directory

A cloud-based suite of identity management capabilities that enables you to securely manage access to Azure services and resources for your users

Provides application management, authentication, device management, and hybrid identity

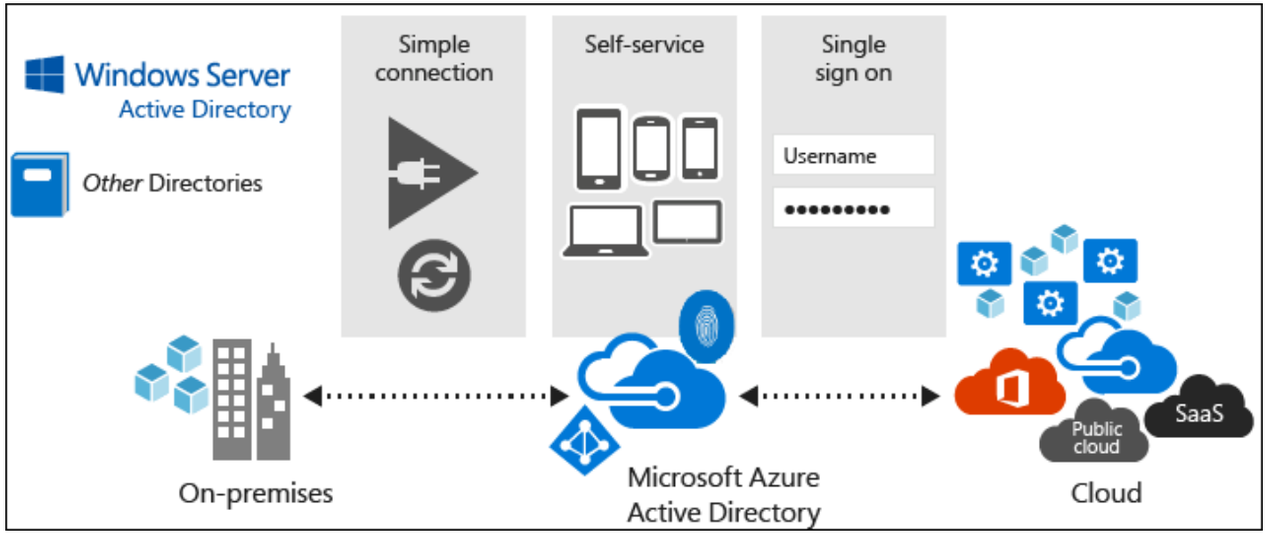


What is Azure Active Directory? - https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis

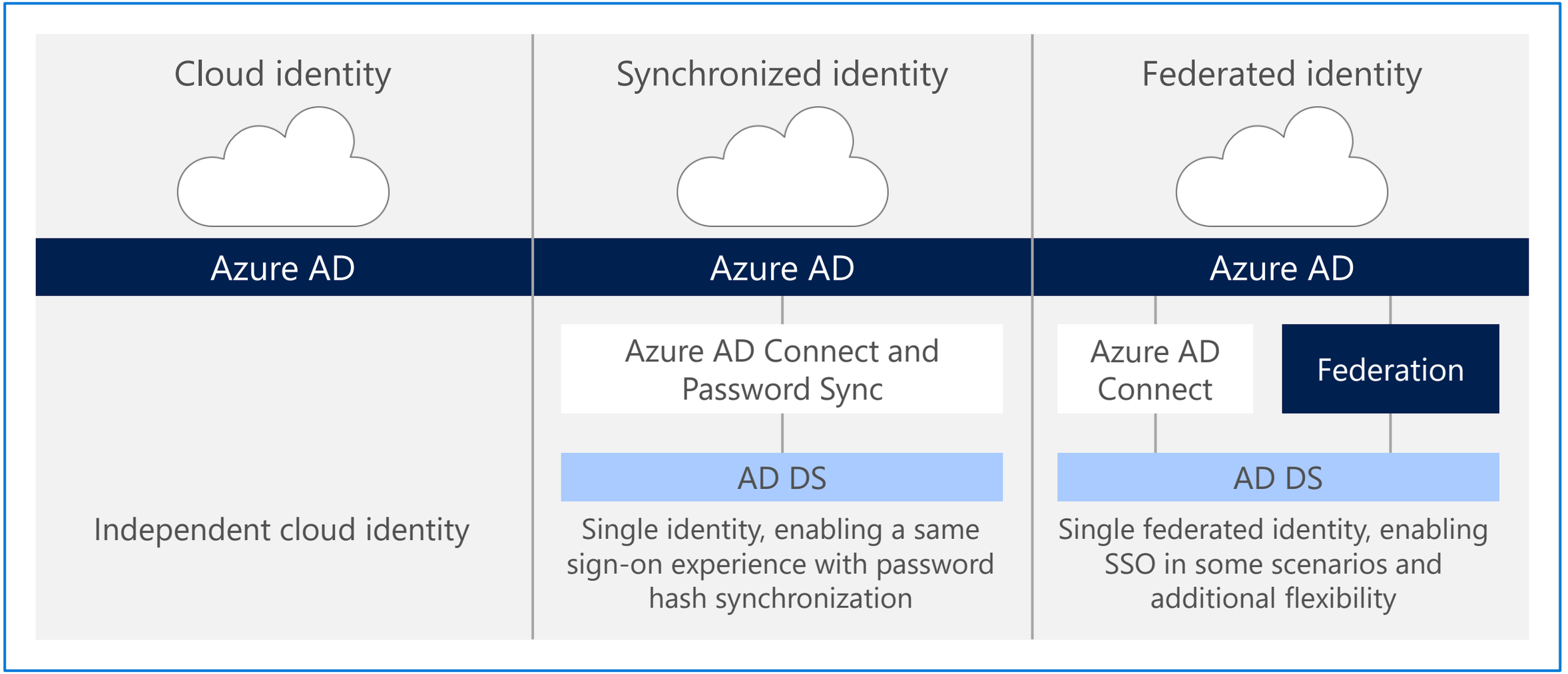
Azure AD advantages

- Azure Active Directory (Azure AD) operates as a Microsoft-managed directory service in the cloud (PaaS)
- You can use Azure AD to:

  - Configure access to applications
  - Configure single sign-on (SSO) to cloud-based SaaS applications
  - Manage users and groups
  - Provision users
  - Enable federation between organizations
  - Provide an identity management solution
  - Identify irregular sign-in activity
  - Configure multi-factor authentication (MFA)
  - Extend existing on-premises Active Directory implementations to Azure AD
  - Configure Application Proxy
  - Configure Conditional Access



Azure AD Authentication and provisioning options



Azure AD recommended actions

Recommended action	Detail
Enable Security Defaults	Protect all user identities and applications by enabling MFA and blocking legacy authentication
Enable Password Hash Sync (if using hybrid identities)	Provide redundancy for authentication and improve security (including Smart Lockout, IP Lockout, and the ability to discover leaked credentials.)
Enable ADFS smart lock out (If applicable)	Protects your users from experiencing extranet account lockout from malicious activity.
Enable Azure Active Directory smart lockout (if using managed identities)	Smart lockout assists in locking out bad actors who are trying to guess your users' passwords or use brute-force methods to get in.
Integrate supported SaaS applications from the gallery to Azure AD and enable Single sign on	Azure AD has a gallery that contains thousands of pre-integrated applications. Some of the applications your organization uses are probably in the gallery accessible directly from the Azure portal. Provide access to corporate SaaS applications remotely and securely with improved user experience (SSO)
Automate user provisioning and deprovisioning from SaaS Applications (if applicable)	Automatically create user identities and roles in the cloud (SaaS) applications that users need access to. In addition to creating user identities, automatic provisioning includes the maintenance and removal of user identities as status or roles change, increasing your organization's security.
Enable Secure hybrid access: Secure legacy apps with existing app delivery controllers and networks (if applicable)	Publish and protect your on-premises and cloud legacy authentication applications by connecting them to Azure AD with your existing application delivery controller or network.
Enable self-service password reset (applicable to cloud only accounts)	This ability reduces help desk calls and loss of productivity when a user cannot sign into their device or an application.
Use non-global administrative roles where possible	Give your administrators only the access they need to only the areas they need access to. Not all administrators need to be global administrators.
Enable Microsoft's password guidance	Stop requiring users to change their password on a set schedule, disable complexity requirements, and your users are more apt to remember their passwords and keep them something that is secure.

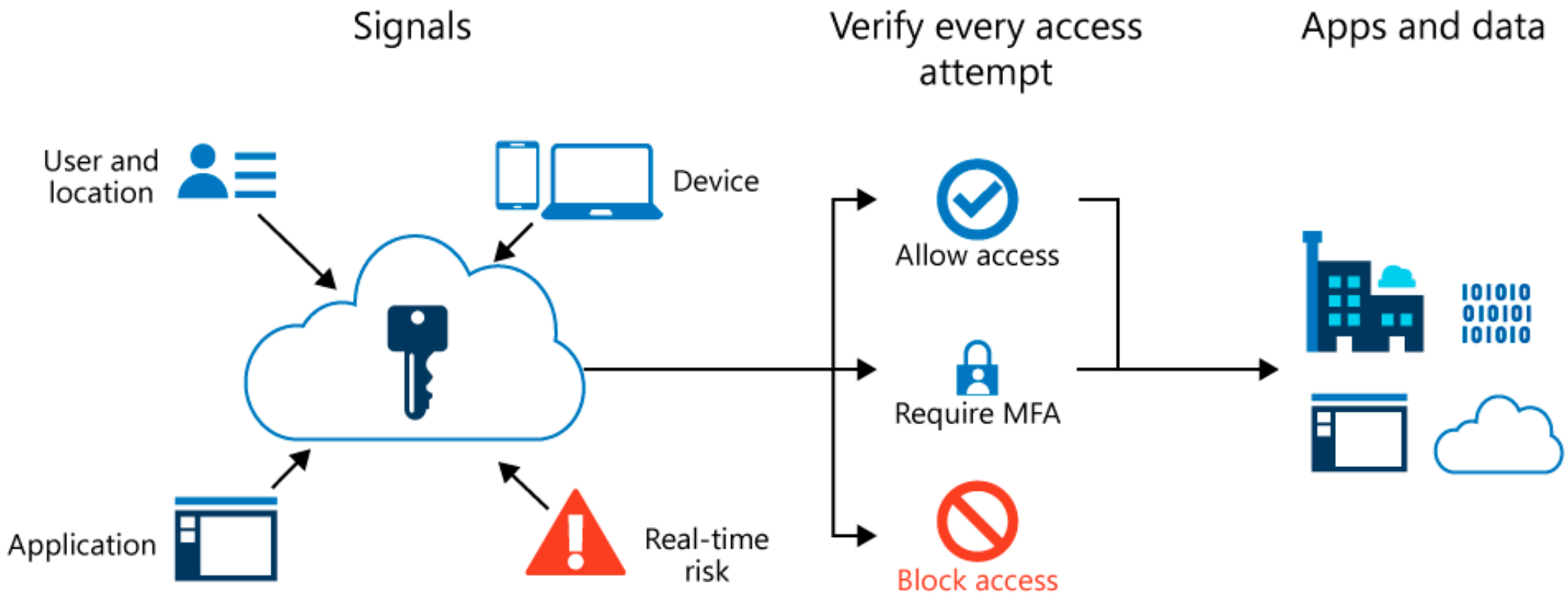
Multi-Factor Authentication

- Multi-Factor Authentication (MFA) in Azure AD helps increase security by requesting users provide a username and a password when signing in and then using a second authentication method

- The second authentication method might be acknowledging:
  - A randomly generated pass code
  - A phone call
  - A phone SMS
  - A smart card (virtual or physical)
  - A biometric device
  - An OATH hardware token

Conditional Access

Conditional Access brings signals together, to make decisions, and enforce organizational policies.



Azure AD Secure Access

Conditional Access

Multi-Factor Authentication

Secure Access

Require Azure Active Directory Premium P1

Azure AD Smart Lockout

- Smart Lockout locks out bad actors who are trying to guess your users' passwords or use brute-force methods to log into your system.
- By default, after 10 failed sign-in attempts, Smart Lockout locks the account from sign-in attempts for one minute.
- Smart Lockout uses "familiar location versus unfamiliar location" algorithms to differentiate between a bad actor and the genuine user.

Access Reviews

- Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and privileged role assignments
- With access reviews, Microsoft 365 Global admins and User Account admins can perform the following tasks:
  - Evaluate guest user access
  - Evaluate employee access to applications and group memberships
  - Collect access review controls into programs that are relevant
  - Recertify the role assignment of administrative users who are assigned to Azure AD roles

https://www.ictpower.it/guide/configurare-le-verifiche-degli-accessi-access-reviews-ad-azure-ad-e-a-microsoft-365.htm

Require Azure Active Directory Premium P2

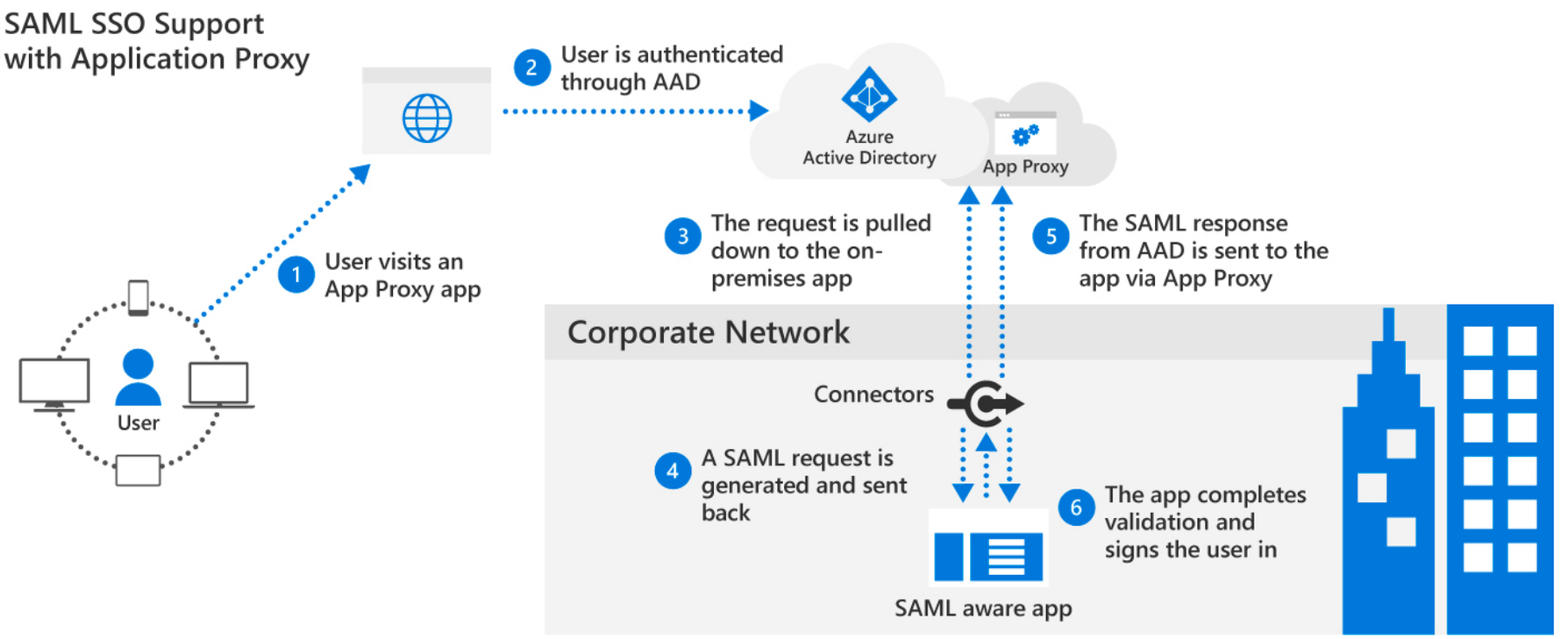
Azure AD Privileged Identity Management

- Azure AD Privileged Identity Management enables you to manage, control, and monitor access within your organization
- Azure AD Privileged Identity Management helps your organization:
  - See which users are assigned privileged roles to manage Azure resources, as well as which users are assigned administrative roles in Azure AD
  - Enable on-demand, "just in time" administrative access to Microsoft Online Services
  - Get alerts about changes in administrator assignments
  - Require approval to activate Azure AD privileged admin roles
  - Review membership of administrative roles

https://www.ictpower.it/guide/configurare-laccesso-sicuro-ad-azure-ad-utilizzando-privileged-identity-management.htm

Require Azure Active Directory Premium P2

Azure AD Application Proxy



https://www.ictpower.it/sistemi-operativi/pubblicare-remote-desktop-services-e-remoteapp-utilizzando-azure-ad-application-proxy.htm

Require Azure Active Directory Premium P1

DEMO

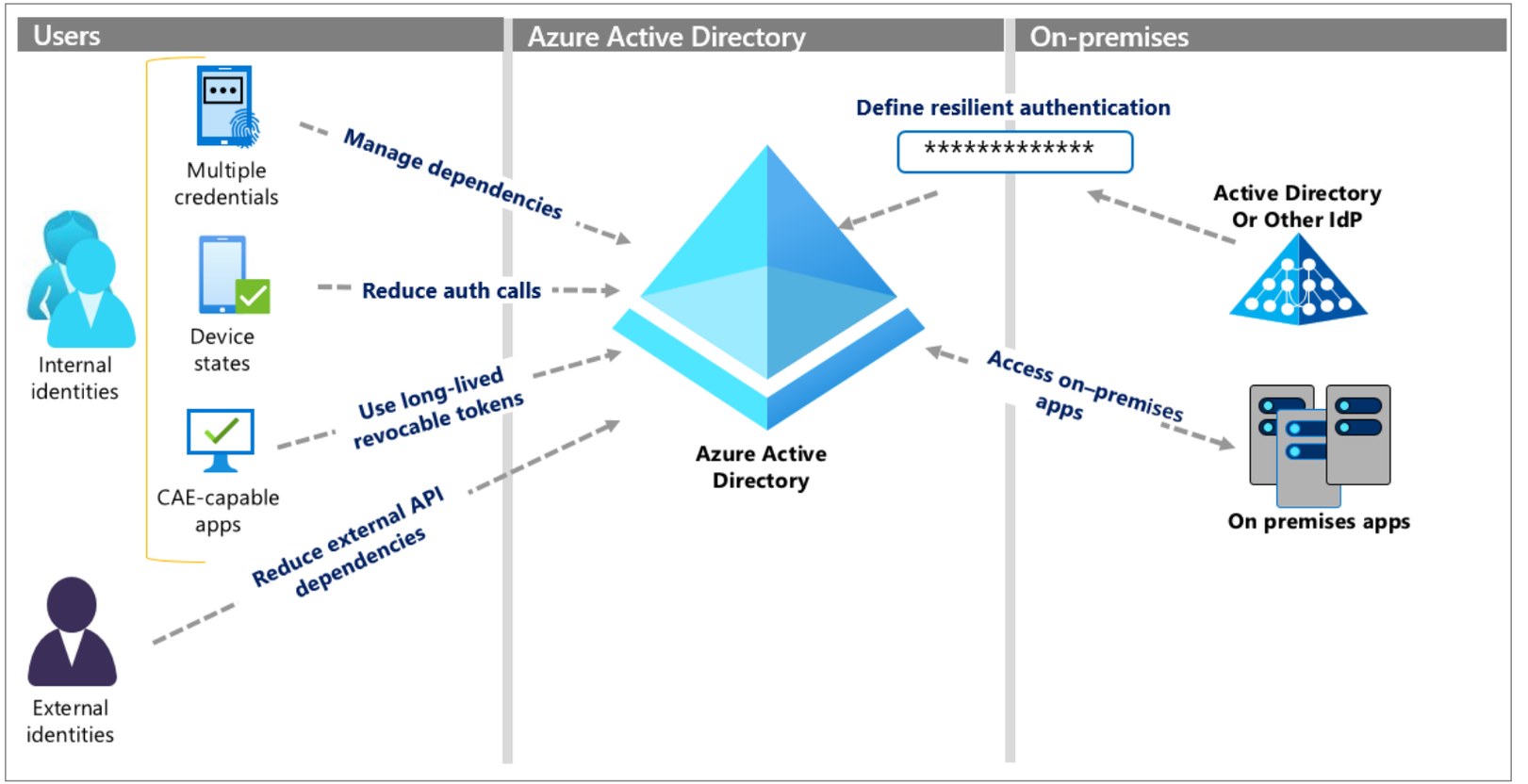
Building resilience into Identity and Access Management (IAM) with Azure AD

Identity and access management (IAM) is a framework of processes, policies, and technologies that facilitate the management of identities and what they access. It includes the many components supporting the authentication and authorization of user and other accounts in your system.

In the context of your identity infrastructure, resilience is the ability to endure disruption to services like authentication and authorization, or failure of other components, with minimal or no impact to your business, users, and operations. The impact of disruption can be severe, and resilience requires diligent planning.

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/resilience-in-infrastructure

Ways to increase resilience in Azure AD



- Build resilience with credential management
- Build resilience with device states
- Build resilience by using Continuous Access Evaluation (CAE)
- Build resilience in external user authentication
- Build resilience in your hybrid authentication
- Build resilience in application access with Application Proxy

ICT POWER.IT

Microsoft

Grazie

/NicolaFerrini.it

@nicolaferrini