2018 Global Azure BOOTCAMP

CloudGen
ominidi verso l'evoluzione

2018

Global Azure

BOOTCAMP

VERONA

Gli sponsor Mondiali

2018 Global Azure BOOTCAMP

CloudGen ominidi verso l'evoluzione

opsgility

JET BRAINS

SERVICEBUS360

Microsoft

myget

cerebrata

CloudMonix

Gli sponsor del nostro evento

Platinum Sponsor

Gli sponsor del nostro evento

Gold Sponsor

Gli sponsor del nostro evento

2018 Global Azure BOOTCAMP

CloudGen ominidi verso l'evoluzione

digital joy

dgroove Tecnologia emozionale.

Basic Sponsor

Tweet della giornata

#GlobalAzure

@cloudgen_verona

CloudGen

2018
Global Azure
BOOTCAMP

ARGOMENTO

Azure Active Directory

hybrid identity & security

Alessandro Appiani

Founder & CTO - Pulsar IT

@AlexAppiani

alessandro.appiani@pulsarit.net

https://www.linkedin.com/in/alexappiani

Alessandro Appiani - about me

- 30+ years experience in IT Technologies and Solutions
- Computer Science Master’s Degree (full marks with honors) in 1989
- Founder of Italian Association for Artificial Intelligence in 1988
- Microsoft Certified since 1995
- Microsoft TechNet speaker & Train-the-trainer since 1996
- MVP, MCT, MCITP Windows+Exchange+Lync+Office365
  - Microsoft Most Valuable Professional Skype for Business (Office Servers)
  - Microsoft Windows Expert since version NT 3.51 (1995)
  - Microsoft Exchange Expert since first product release (Exchange 4.0 - 1996)
  - Microsoft Lync/Skype Expert since first product release (LCS 2003)
  - Microsoft Office 365 Expert since first Cloud version (BPOS - 2009)
- Pulsar IT Founder & CTO
  - advisory, architectures, technologies, digital transformation, ...
- Twitter: @AlexAppiani

Microsoft® MVP Most Valuable Professional

Skype for Business
Office Servers

PULSAR

the best way to get
value from IT

Design, Deploy, and Support Microsoft Solutions

Microsoft Excellence since 1995

www.pulsarit.net

Microsoft Partner

Microsoft

Gold Communications
Gold Messaging
Gold Datacenter
Gold Cloud Productivity
Gold Windows and Devices
Silver Cloud Platform
Silver Collaboration and Content
Silver Application Development

Enterprise Collaboration
Teams, OneDrive, SharePoint,
Skype, Exchange, Office 365 Apps

Telephony & Enterprise Voice
Skype for Business Telephony,
Microsoft's Phone System / Cloud PBX

Smart Working & Devices
Trusted environment for Smart Productivity

Modern & Hybrid DataCenter
Azure, Windows Server, Hyper-V, System Center

Enterprise Mobility + Security
PC e Device Management, Mobile Application Management,
(Hybrid) Identity-based Security

www.pulsarit.net – info@pulsarit.net

Agenda

- Identity & Directory basics
- Azure Active Directory
- Hybrid Identity
  - Architecture
  - User Sign-In Options
  - Azure AD Connect
- Modern Authentication
- Azure Identity Power

BASICS

Fundamentals and Terminology

Identity

- A (digital) identity is information on an entity used by computer systems to represent an external agent. That agent may be a person, organisation, application, or device. [1]
- ISO/IEC 24760-1 defines identity as "set of attributes related to an entity" [2]
- The identity information makes each entity unique and different from each other
- Identity are usually stored in a repository (ie. a Directory)
- From a security point of view each identity information in the repository represents a Security Principal used to uniquely identify an entity (ie: User Account)

[1] Digital Identity
https://en.wikipedia.org/wiki/Digital_identity

[2] ISO/IEC 24760-1:2011 Information technology -- Security techniques -- A framework for identity management -- Part 1: Terminology and concepts
https://www.iso.org/standard/57914.html

Authentication

- Authentication is a process for verifying the identity of something or someone
- Authentication relies on trust among process components
  - customs, passports, identity card, issuing organizations, people, ...
- And on validity and integrity of credentials

Authorization

- Is the process to gain access to resources, usually with different rights for different identities
- Identity is verified thru authentication
- Security administrator of resource define what kind of rights a known entity has or what type of actions are permitted

IDENTITY & DIRECTORY

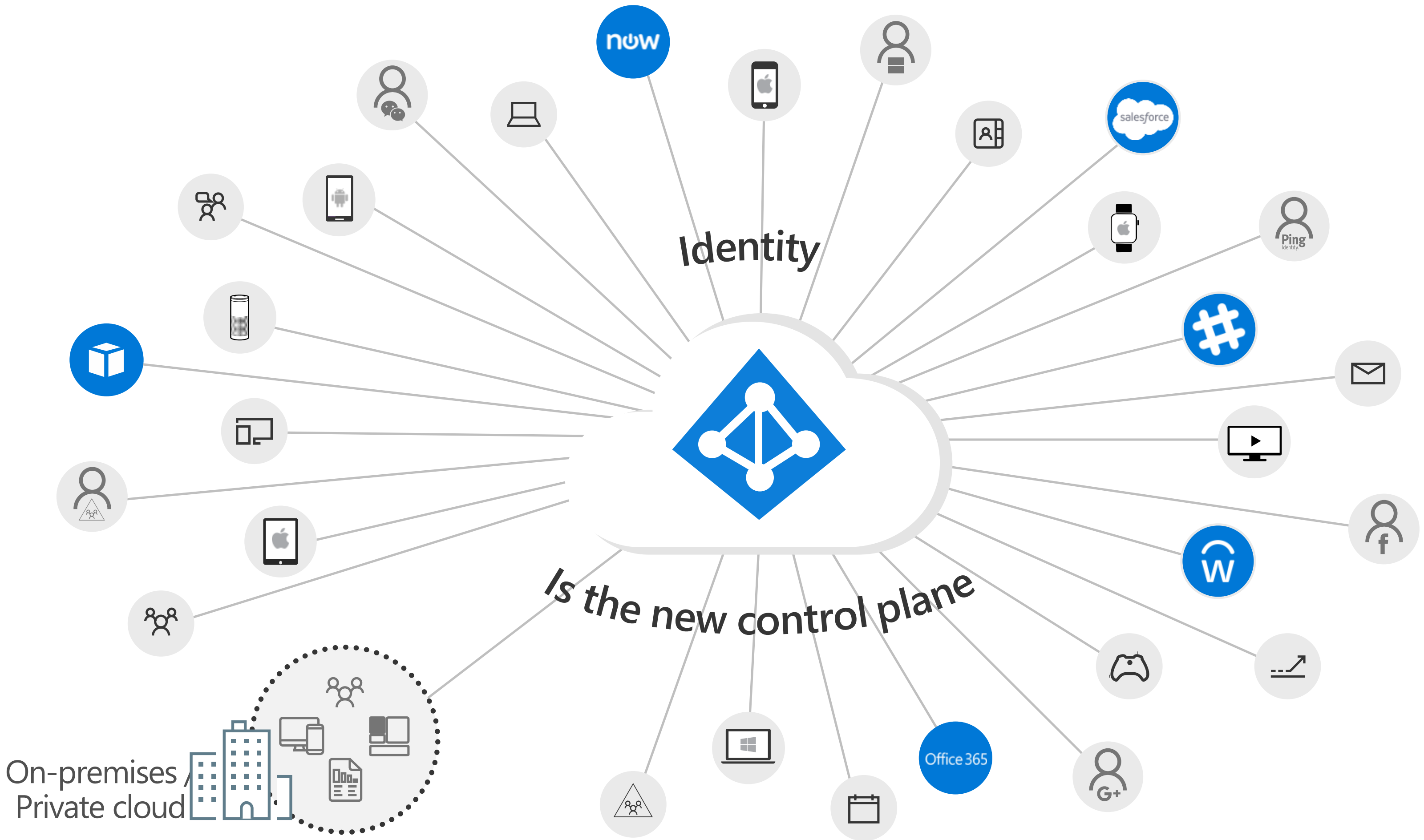
Identity in Microsoft World: Active Directory

- Active Directory is a Directory Services
- Previewed in 1999 and released in Windows 2000
  - developed based on Microsoft Exchange implementation of X.500 Directory Services (Jet DB, Multi-master, ...) used since March 1996 (v4.0)
- Starting Windows Server 2008 other services were added
  - ie: Active Directory Federation Services
- On July 2012 Microsoft announced developer preview of Azure Active Directory (AAD)
- AAD is a multi-tenant, cloud-based, directory and identity management services

Azure AD is now the backplane for Identity & Security of all Azure/Office 365 Platform

2018 Global Azure BOOTCAMP

CloudGen



Azure Active Directory (AAD)

The Office 365 Directory

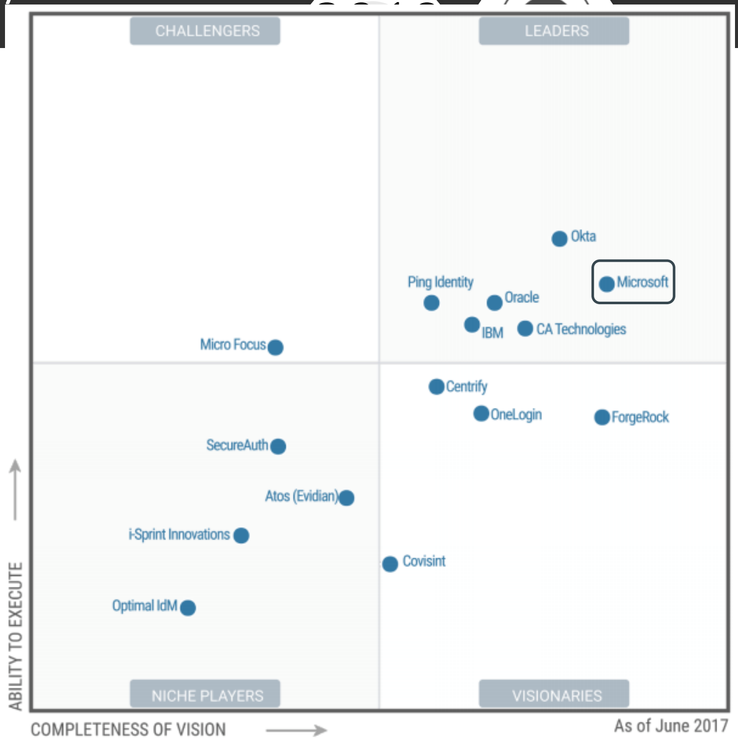
Identity in Microsoft Clouds

- Office 365
  - started with his own directory “Organizational identity” (based on “hidden” underlying Azure AD)
  - 2013 tenant version introduced Organizational identity, Hybrid Models, Active Directory federation and Sync with on-premises - preview 2012, GA March 2013
    - http://blogs.office.com/b/microsoft_office_365_blog/archive/2013/02/27/office-365-commercial-availability-global-customers.aspx
- Azure
  - started with Microsoft ID (Live ID) and Application Identity only (managed by Developers)
  - IaaS introduced Active Directory integration - preview July 2012, GA Nov 2012
    - http://blogs.msdn.com/b/windowsazure/archive/2012/07/12/announcing-the-developer-preview-of-windows-azure-active-directory.aspx
    - http://blogs.msdn.com/b/windowsazure/archive/2012/11/28/windows-azure-now-supports-federation-with-windows-server-active-directory.aspx
  - Active Directory enhancements: Multi-AD Management, Multi-Factor Authentication, ... - Sept 2013
    - http://weblogs.asp.net/scottgu/archive/2013/09/26/windows-azure-new-virtual-machine-active-directory-multi-factor-auth-storage-web-site-and-billing-improvements.aspx
- Azure AD is now the backplane for Identity & Security of all Azure Platform

Azure Active Directory

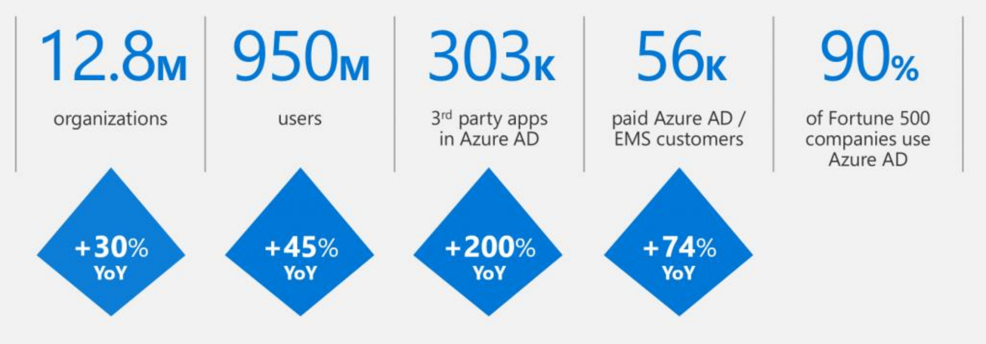
Every Office 365 and Microsoft Azure customer uses Azure Active Directory

- Microsoft “Identity Management as a Service (IDaaS)” for organizations
- Millions of independent identity systems controlled by enterprise and government “tenants”
- Information is owned and used by the controlling organization—not by Microsoft
- Born-as-a-cloud directory for Office 365. Extended to manage across many clouds
- Evolved to manage an organization’s relationships with its customers/citizens and partners (B2C and B2B)



Source: Gartner (June 2017)

Gartner Magic Quadrant for Access Management 2017



12.8M organizations +30% YoY

950M users +45% YoY

303K 3rd party apps in Azure AD +200% YoY

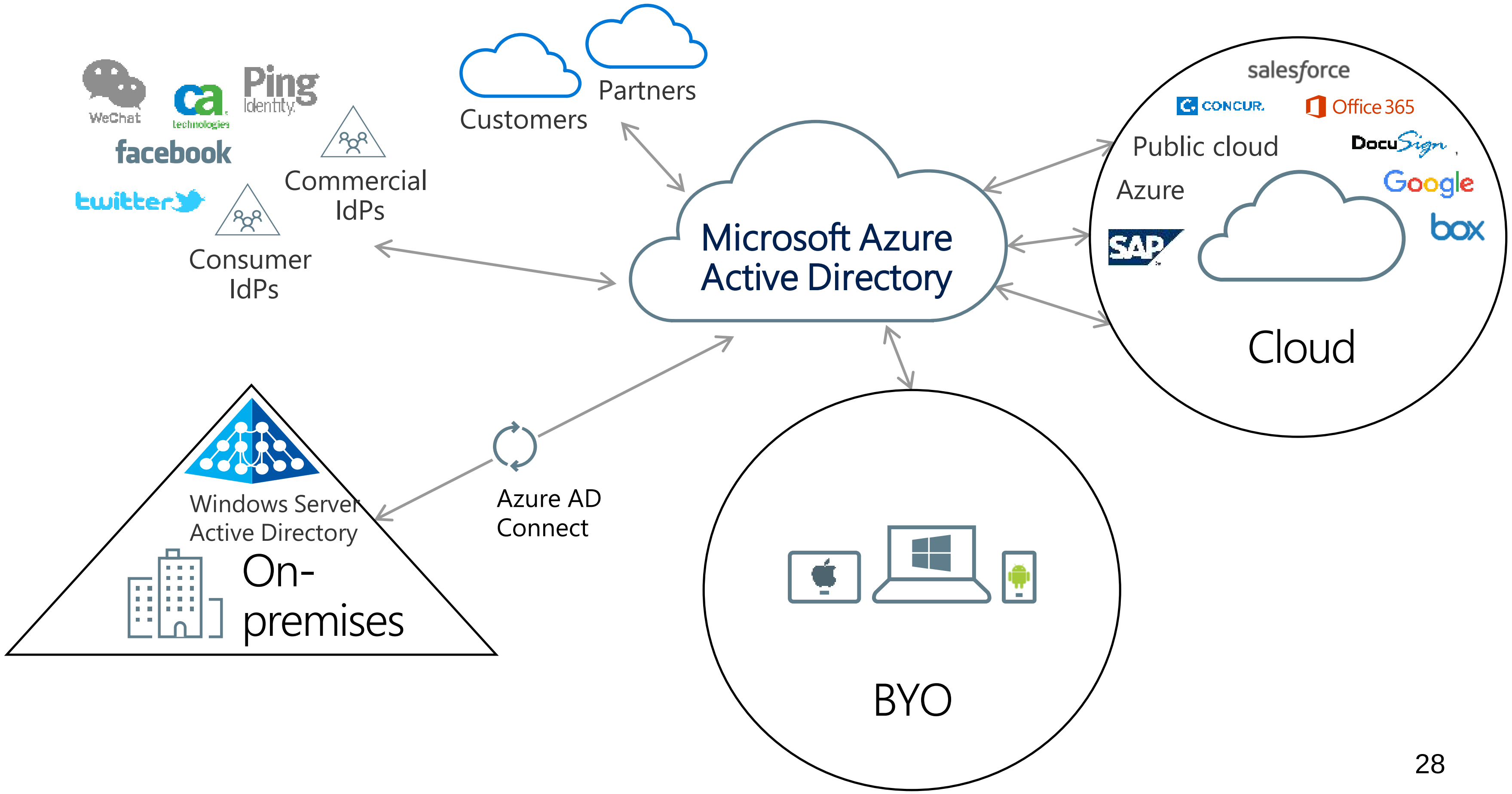
56K paid Azure AD / EMS customers +74% YoY

90% of Fortune 500 companies use Azure AD

October-2017 Usage Data

Azure AD & Identity as the Control Plane

- Azure AD is the Microsoft Active Directory investments target for new features
- «Cloud-First» ☺



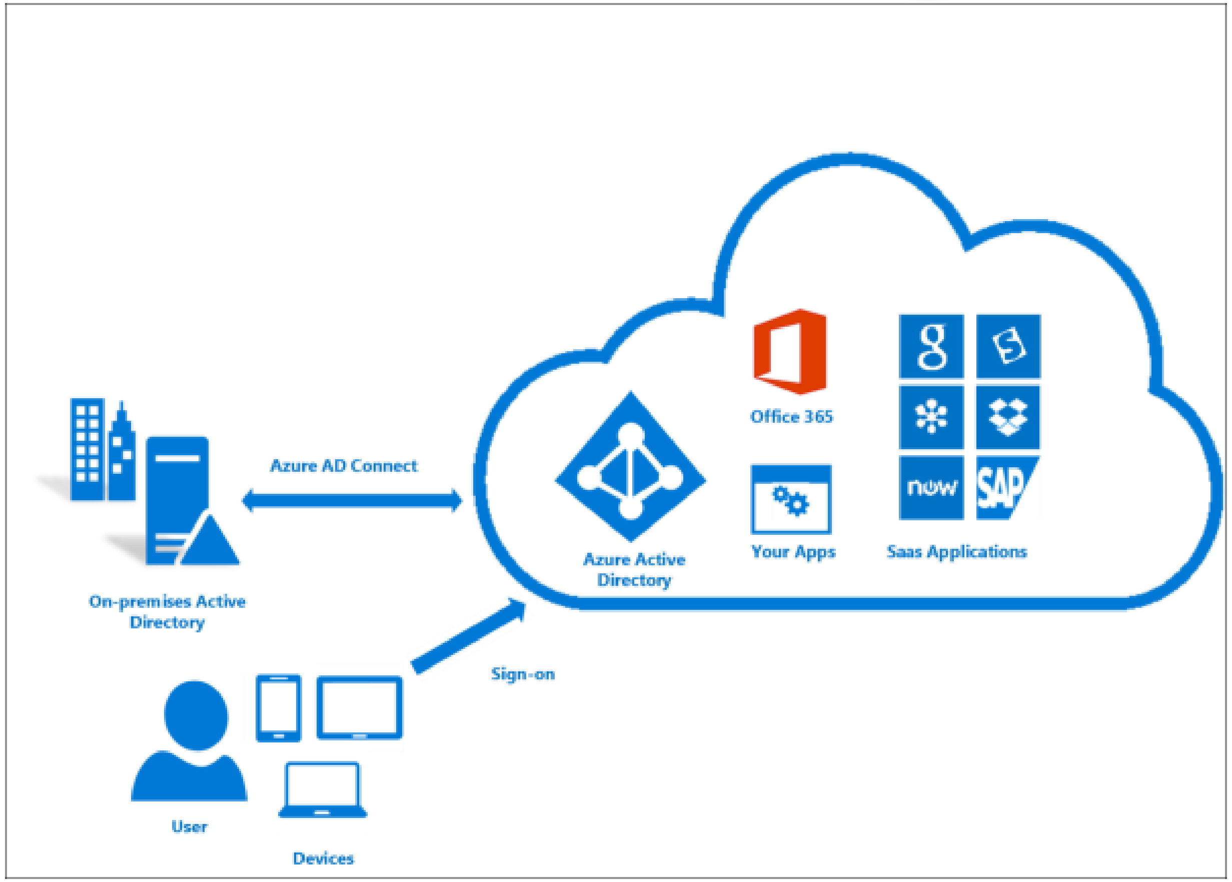
Hybrid Identity

Hybrid Identity concept

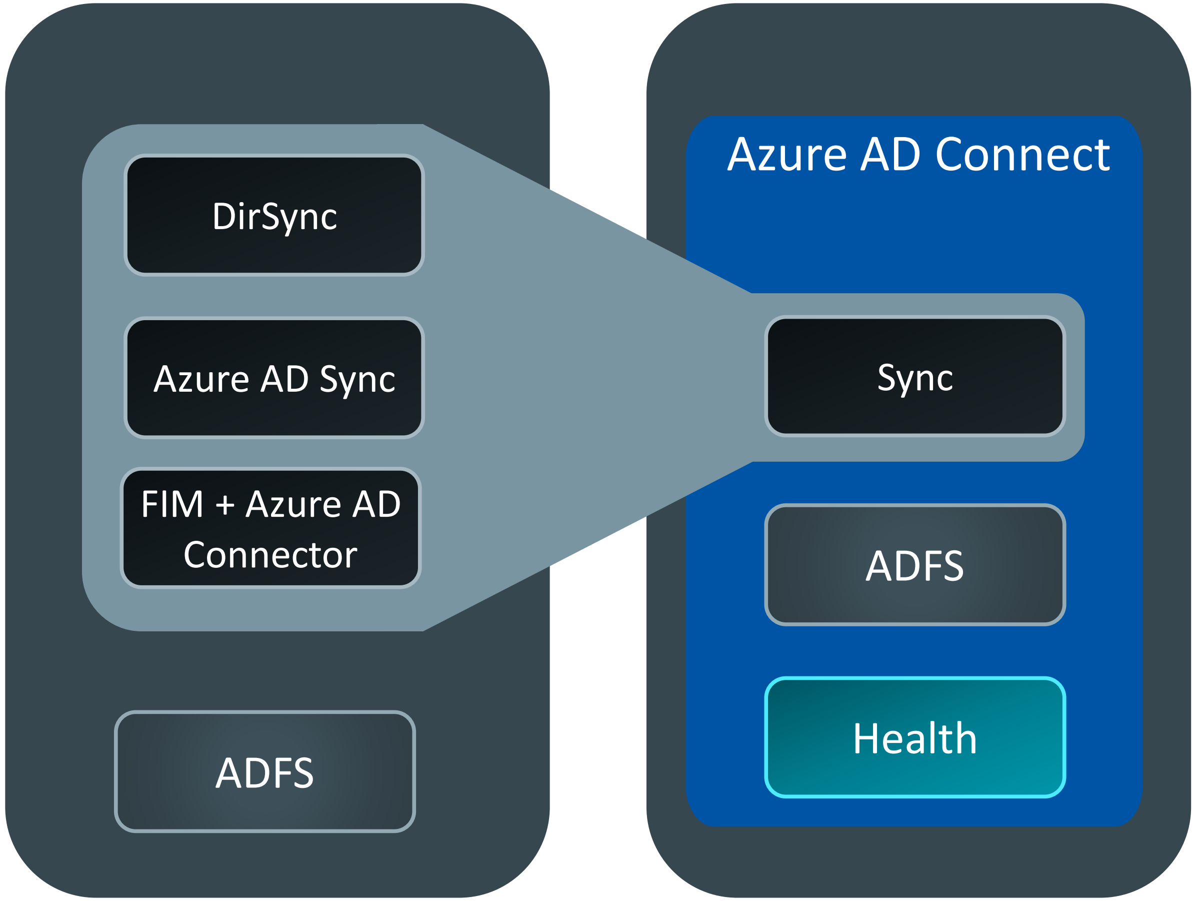
- More than one Identity and Directory involved
  - usually (one or more) Directory on-prem (ie: AD Forests) and (one) Directory in cloud (Azure AD Tenant)
- We want to "share" and use the same Identity (ie: User Account and Password), and not have two distinct ones
- Identities (set of attributes) have to be replicated among Dirs
  - two way sync is possible ("Writeback" from Cloud to OnPrem)
- Identity - Authentication - Authorization
  - different concepts and processes
  - Azure AD Connect does not manage Authentication (user sign-in)

Components

- Azure AD Connect
  - a tool to provision and configure hybrid identity components
- Azure AD Connect Sync Engine
  - the replication engine between AD and Azure AD (and viceversa)
  - sync identities and attributes between directories
- Sign-in
  - the authentication process required to access (Cloud) resources



What is Azure AD Connect?



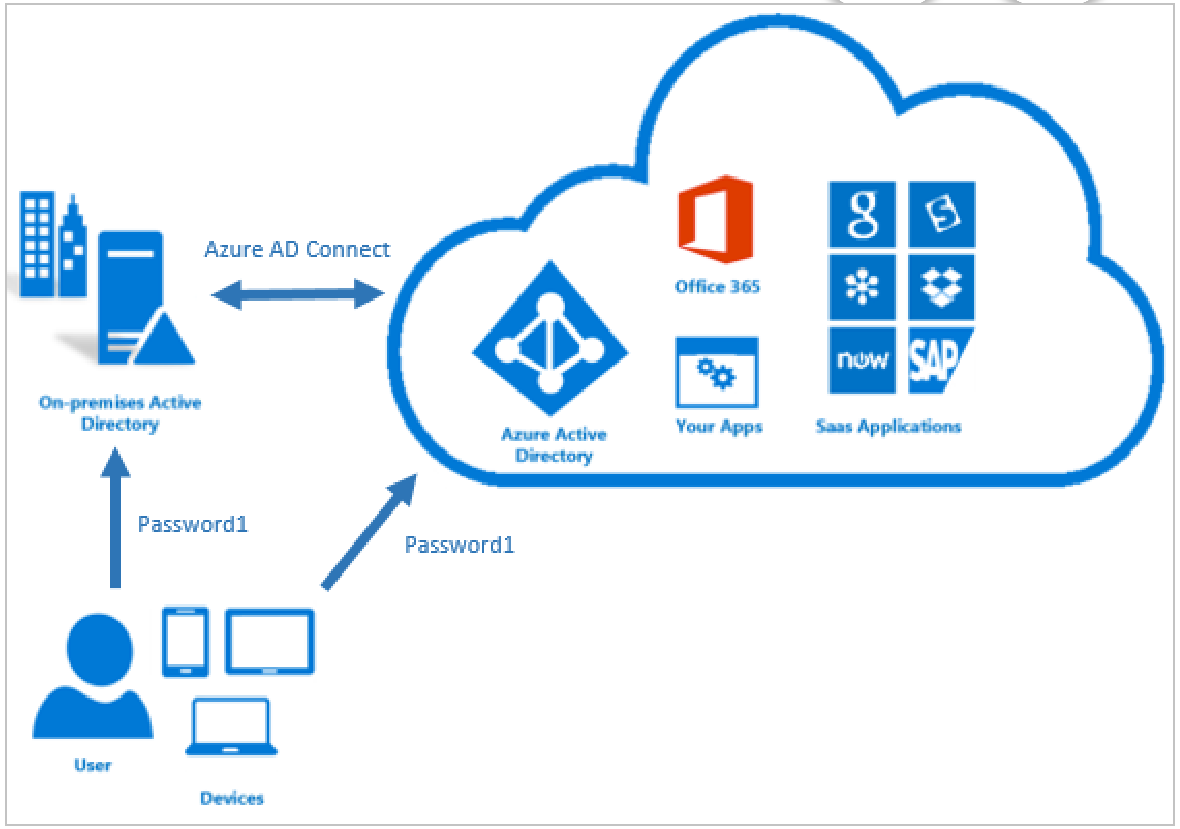
- Primary tool to onboard to Azure AD
- Express Settings gets customers connected in a matter of minutes
- Provides install & configuration of Sign-in Options components

Hybrid Identity Sign-in Options

- Syncronized
  - Password hash synchronization (PHS)
- Pass-through
  - Pass-Through Authentication (PTA)
- Federated
  - Active Directory Federation Services (ADFS)
  - Third Party (Ping, Centrify, Okta, OneLogin, ...)

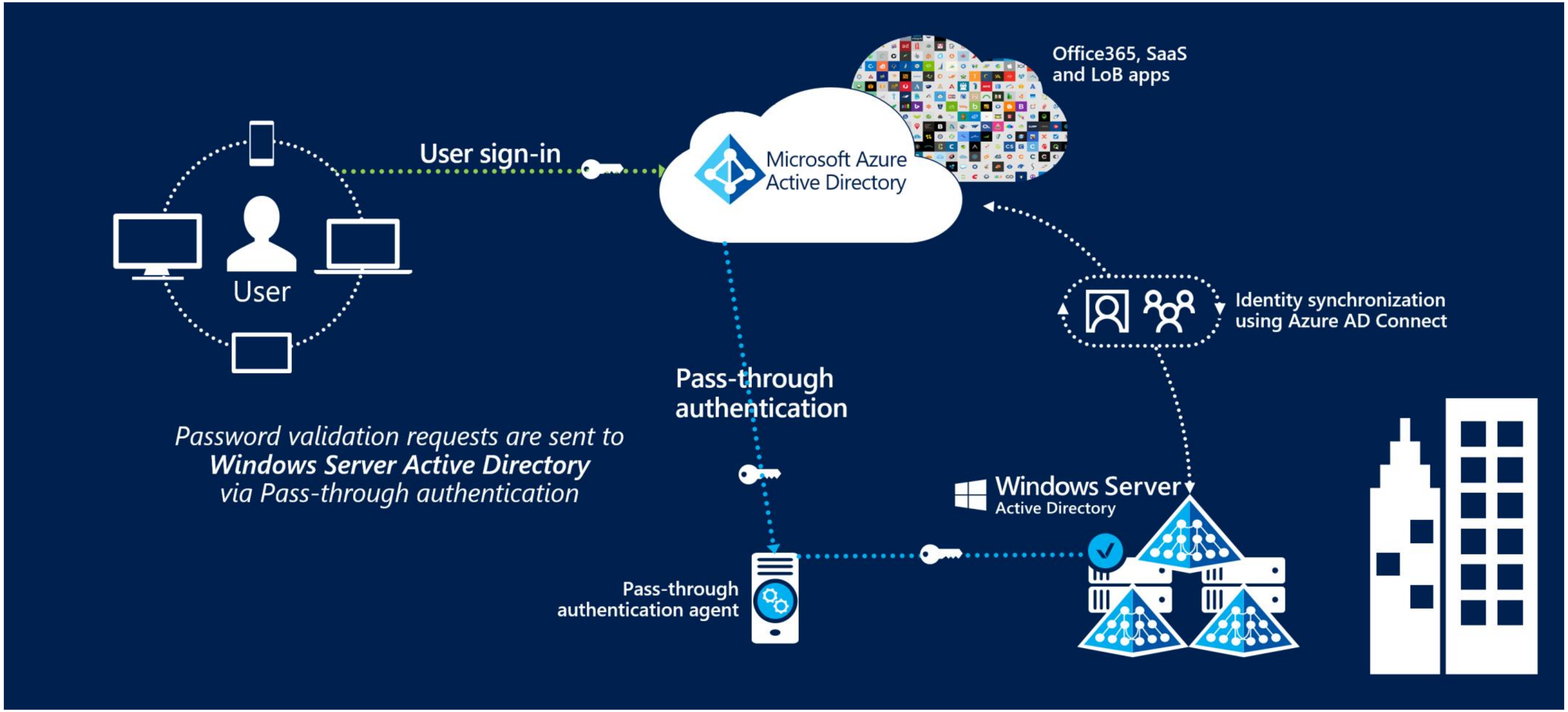
Password Hash Sync (PHS)

- The easiest way to Hybrid identity
- The original clear text password is never accessed nor replicated (hash does)
- The same password is used to authenticate both on-prem and cloud



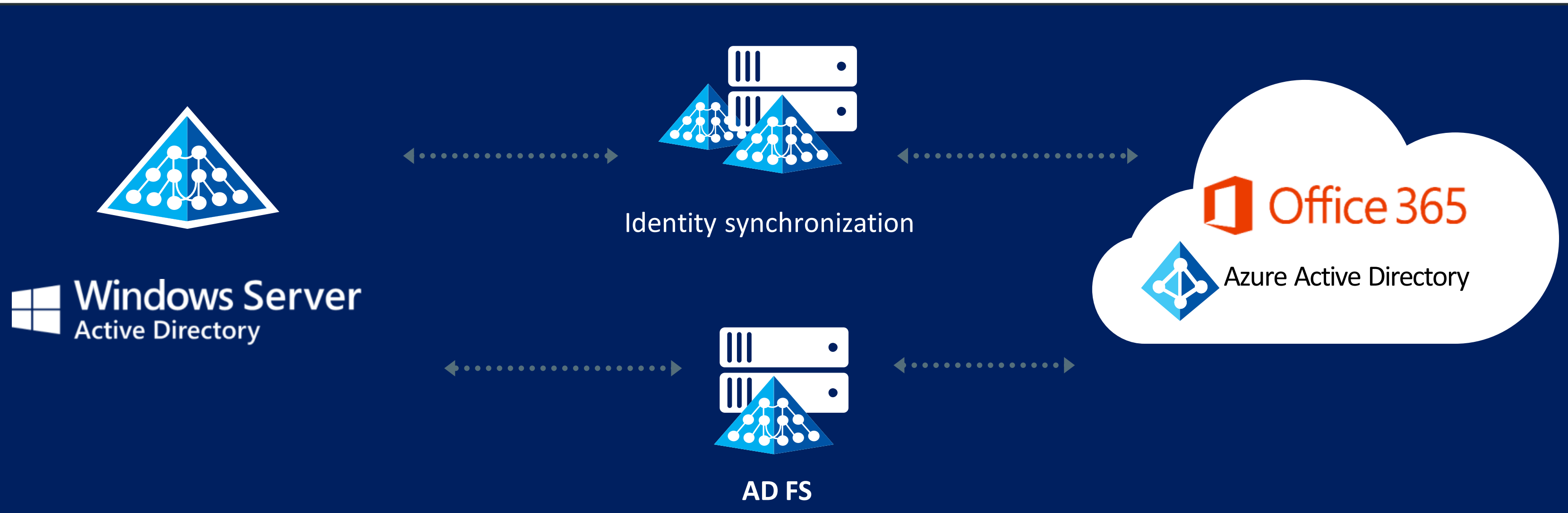
Pass-Through Authentication (PTA)

- Enables on-premises passwords validation without complexity



Password validation requests are sent to ***Windows Server Active Directory*** *via Pass-through authentication*

Active Directory Federation to on premises (ADFS)



User attributes are synchronized using Azure AD Connect; **authentication is passed back through federation** and completed against **Windows Server Active Directory**

End User Experience

All authentication to on premises AD

Seamless single sign on from domain joined PC’s

Password Change Portal

IT Pro / Admin Experience

Azure AD Connect

AD FS and AD FS Proxy (WAP) installed on premises

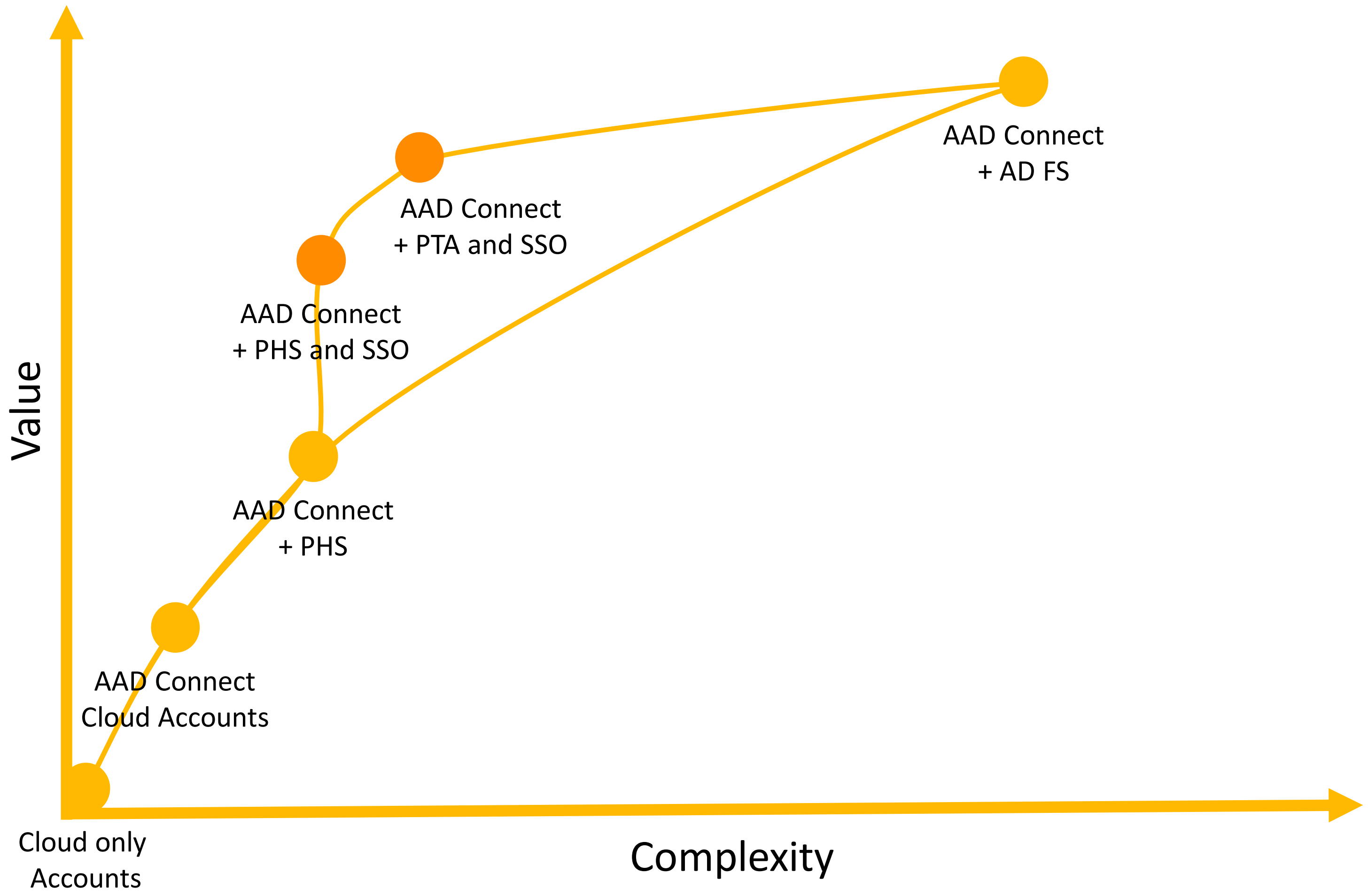
Credentials not stored in Azure AD

Choosing the user sign-in method

I need to	PHS	PTA	ADFS
Sync new user, contact, and group accounts in on-premises Active Directory to the cloud automatically.	x	x	x
Set up my tenant for Office 365 hybrid scenarios.	x	x	x
Enable my users to sign in and access cloud services by using their on-premises password.	x	x	x
Implement single sign-on by using corporate credentials.	x*	x*	x
Ensure that no passwords are stored in the cloud.		x	x
Ensure that passwords are typed only on corporate servers (and not on Microsoft forms/services)			x
Enable Azure AD features (ie: multi-factor authentication, password change, ...) for on-premises applications.			x

* using seamless SSO --- works only with Modern Authentication enabled Apps on Kerberos platform

Sign-in curve

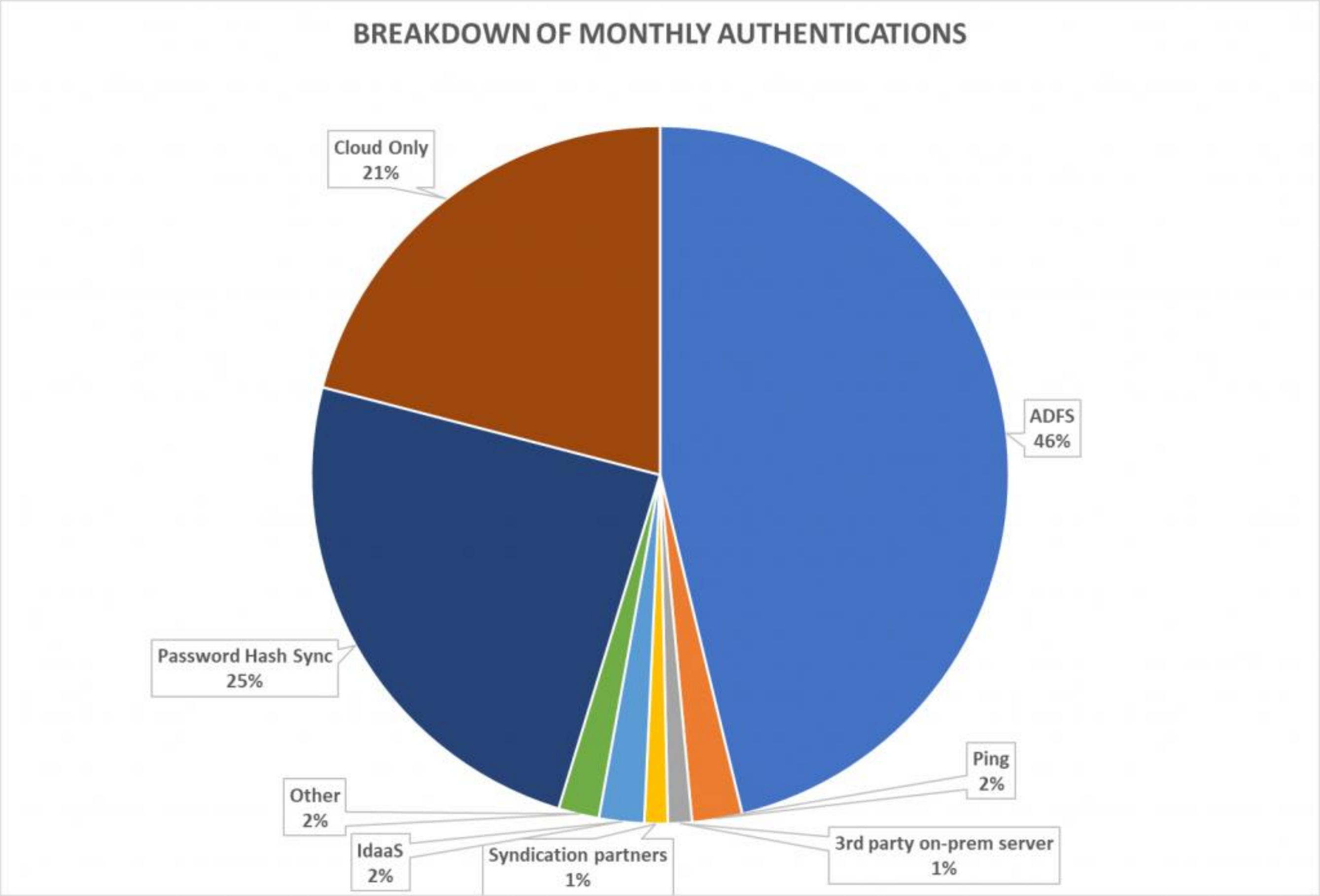


What AD FS offers that PTA with sSSO doesn’t

- Passwords are always in your control boundary - i.e. don’t pass through the cloud
- Support for smartcard / certificate authentication
- Support for 3rd Party MFA providers and integration with On-Premises Applications
- Fine tune authentication behavior for Intranet
- On-premises conditional access rules based on issuance policies, such as
  - Exchange protocols (e.g. pop, imap etc)
  - Inside network claim
- Azure MFA as primary also for On-Premises authentication

Azure AD Authentications

October-2017*



*How organizations are connecting their on-premises identities to Azure AD

https://cloudblogs.microsoft.com/enterprisemobility/2017/11/13/how-organizations-are-connecting-their-on-premises-identities-to-azure-ad/

Hybrid Options Recap - feature detail

Feature summary	PTA + sSSO	PHS + sSSO	ADFS
Authentication against credentials held on-premises	Yes	No	Yes
Single-Sign-On	Yes	Yes	Yes
Passwords remain on premises	Yes	Salted hash synced	Yes
On-premises MFA solution	No	No	Yes
Azure AD MFA	Yes	Yes	Yes
On-premises password policies	Yes	Partial	Yes
On-premises account enable/disable	Yes	Delayed (30 mins)	Yes
On-premises password expired/lockout	Yes	No	Yes
Conditional access	Yes++	Yes++	Yes
Credentials captured from user via Azure AD UI	Yes	Yes	No
Protection against on-premise account lockout	Smart Lockout	N/A	Extranet Lockout
Cost of implementation	Low	Low	High
Scalability/fault tolerance	Cloud scalability	Cloud scalability	Complex
AuthN fails for remote workers if the on-premises Internet connection is down. Requires HA solution.	Yes	No	Yes
On-going maintenance for authentication	Automated	None	Certificate management
Azure AD Connect Health monitoring	Not integrated	Limited	Yes
Azure AD Identity Protection (requires P2 license)	Yes	Yes	No

Demo

- Office 365 Logon (via ADFS - Firefox)
- SSO - Single Sign-On
- ADFS Change Password

MODERN AUTHENTICATION

What is Modern Authentication

- Modern authentication brings Active Directory Authentication Library (ADAL)-based sign-in to Office client apps across platforms (iOS, OS X, Android, Windows)
- Enables sign-in features such as
  - Multi-Factor Authentication (MFA)
  - SAML-based third-party Identity Providers with Office client applications
  - Smart card and certificate-based authentication
- Enables Conditional Access and Identity-based Security
- Removes the need for Outlook to use the basic authentication protocol
- It's based on OAuth

Modern Authentication

- History
  - Twitter, Ma.gnolia, Google
  - “Secure delegated access"
  - OAuth is an open standard
  - Auth 2.0 2012
- Why Enterprises like it?
  - Authenticated against own environment
  - Token-based, No Password

Modern Authentication Client Support

Office client application	Windows	Mac OS X	Windows Phone	iOS	Android
Office clients	Available now for Office 2013 and Office 2016.	Available now for Office 2016. Also available for OneNote 2014.	Available now.	Word, Excel and PowerPoint are available now for both phones and tablets.	Word, Excel and PowerPoint are available now for both phones and tablets.
Skype for Business (formerly Lync)	Included in Office client.	Available now.	Available now. CBA and other modern features not yet supported.	Available now*.	Available now*.
Outlook	Included in Office client.	Available now.	Coming soon.	Available now.	Available now.
OneDrive for Business	Included in Office client.	Available now.	Available now for Windows Phone 8.1.	OneDrive for Business is available now.	OneDrive for Business is available now.
Legacy clients	There are no plans for Office 2010 or Office 2007 to support ADAL-based authentication.	There are no plans for Office for Mac 2011 to support ADAL-based authentication.	There are no plans for Office on Windows Phone 7 to support ADAL-based authentication.	There are no plans to enable older Outlook iOS clients.	There are no plans to enable older Outlook Android clients.

*Not recommended for split domain configuration that includes both Skype for Business Online and Skype for Business Server

Demo

- Credential Manager - ADAL
- Mobile App (no password saved)

AZURE IDENTITY POWER

Leveraging Azure AD as Primary Identity Backplane

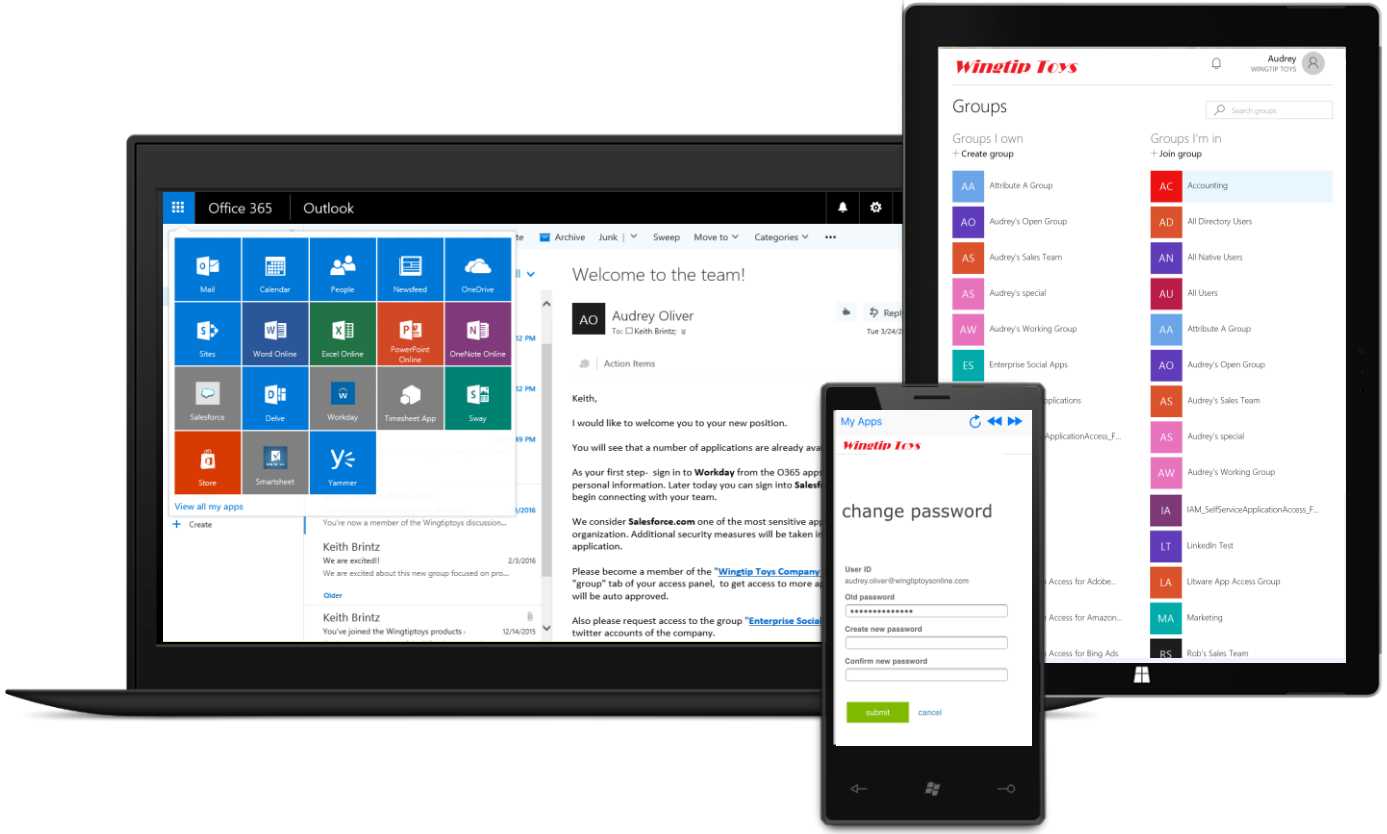
The time has come

- If you enabled Hybrid identity now it's time to go further
- Azure AD as Primary Backplane brings lot of value
  - Self-Service Password Reset
  - Multi-Factor authentication
    - for on-prem apps too with Windows Server 2016
  - Teams and Office 365 Groups
  - Conditional Access
  - Identity-based Security & Protection
  - ...

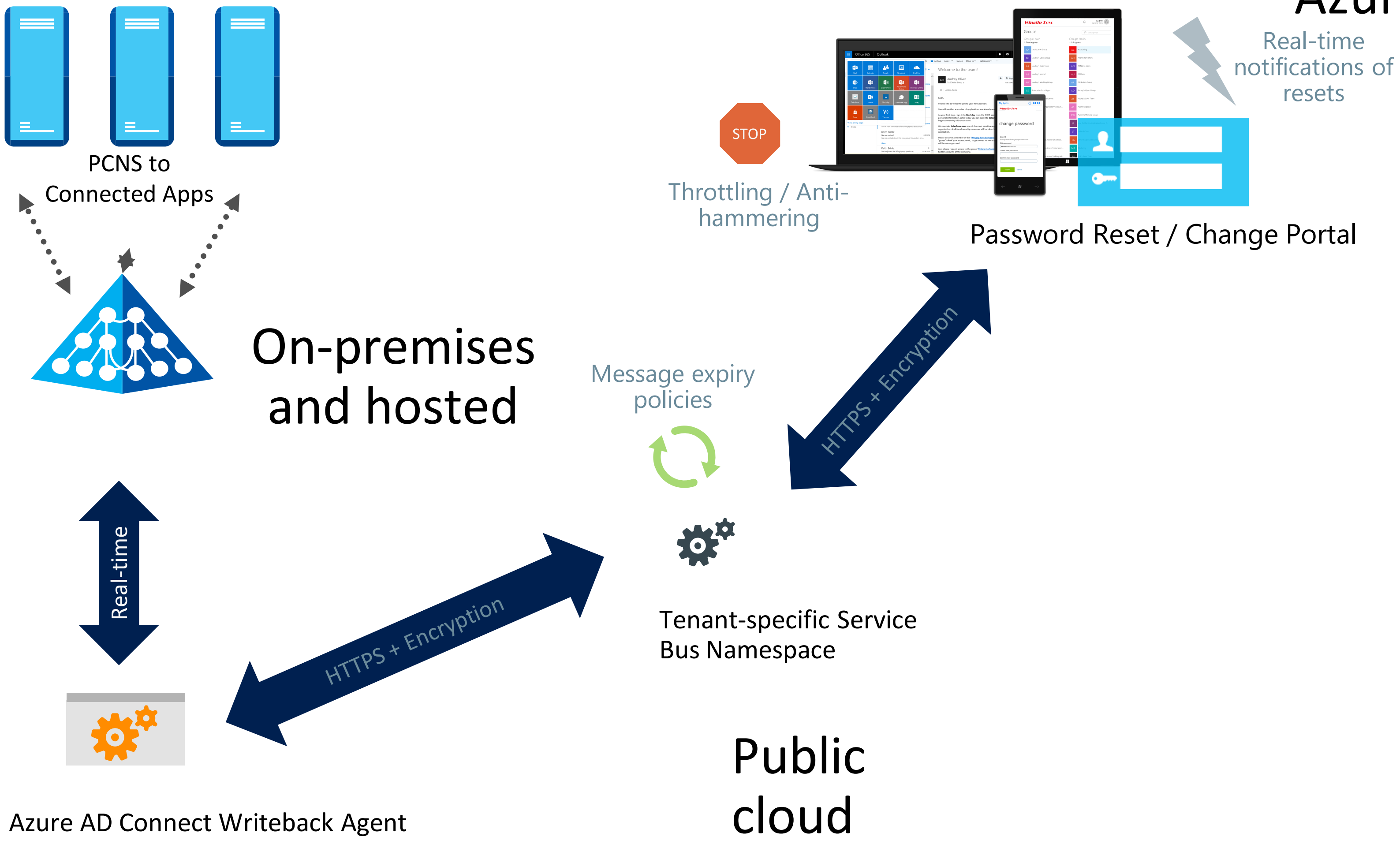
Making the lives of users easier

Integrated end user experiences across devices

- Company-branded, personalized application Access Panel:
  http://myapps.microsoft.com
  + iOS and Android Mobile Apps
- Integrated Office 365 app launching
- Manage your account, apps, and groups
- Self-service password reset
- Application access requests



Self-Service Passwords Management

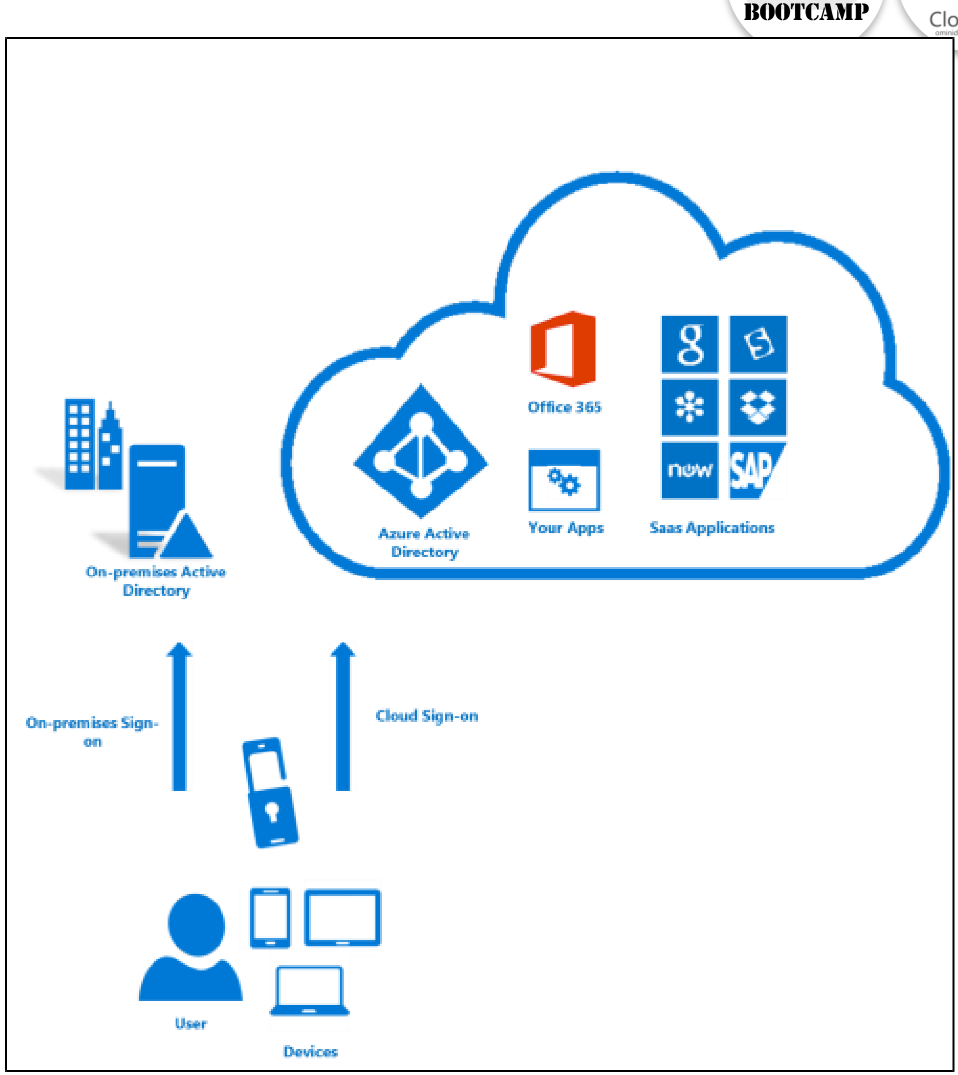


Azure AD Password Management

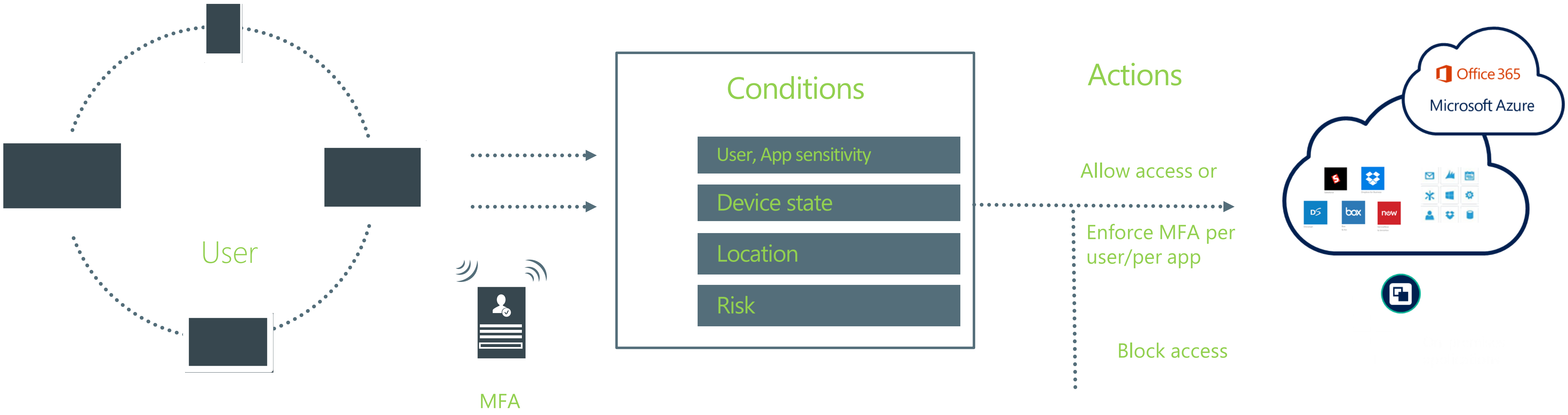
- Works with federation, password sync, or cloud-only user accounts. Enforces all your rich **on-prem password policies**
- Users can **update** their AD passwords or **unlock** their AD accounts in real-time – no waiting for sync
- No poking holes in your corporate firewall requires – all connections occur against port 443 **outbound only**
- Multi-tiered security model:
  - All traffic is over HTTPS
  - Encryption with tenant-specific key
  - Tenant-specific Service Bus namespace for pending requests
  - Integrated anti-hammering, throttling, and message expiry
  - Real-time notifications sent to users and admins

Azure Multi-Factor Authentication (MFA)

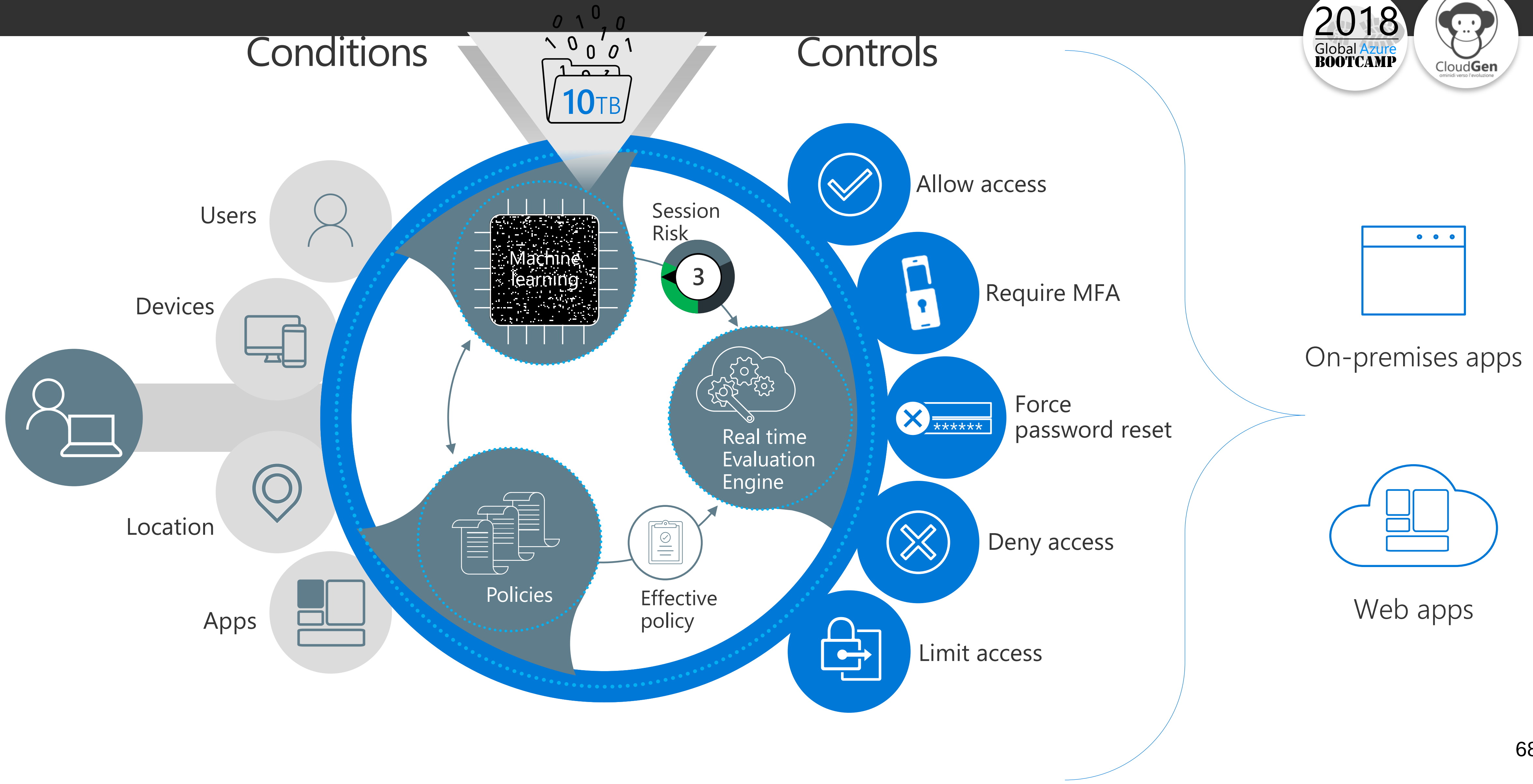
- MFA is Microsoft's two-step verification solution
- It works by requiring any two or more of the following verification methods:
  - Something you know (typically a password)
  - Something you have (a trusted device that is not easily duplicated, like a phone)
  - Something you are (biometrics)



Identity-driven security



Azure Conditional Access



Conditions

Users

Devices

Location

Apps

10TB

Machine learning

Session Risk

3

Real time Evaluation Engine

Policies

Effective policy

Controls

Allow access

Require MFA

Force password reset

Deny access

Limit access

On-premises apps

Web apps

Demo

- MFA
    - Office 365 Admin Portal
- Self-Service Password Reset
- Device Registration
    - Connect-AzureAD
    - Azure Portal

Grazie

Domande?

@AlexAppiani