Identity Management for Hybrid IT with Windows Azure

Microsoft

Maarten Goet

Microsoft MVP

inovativ

MVP

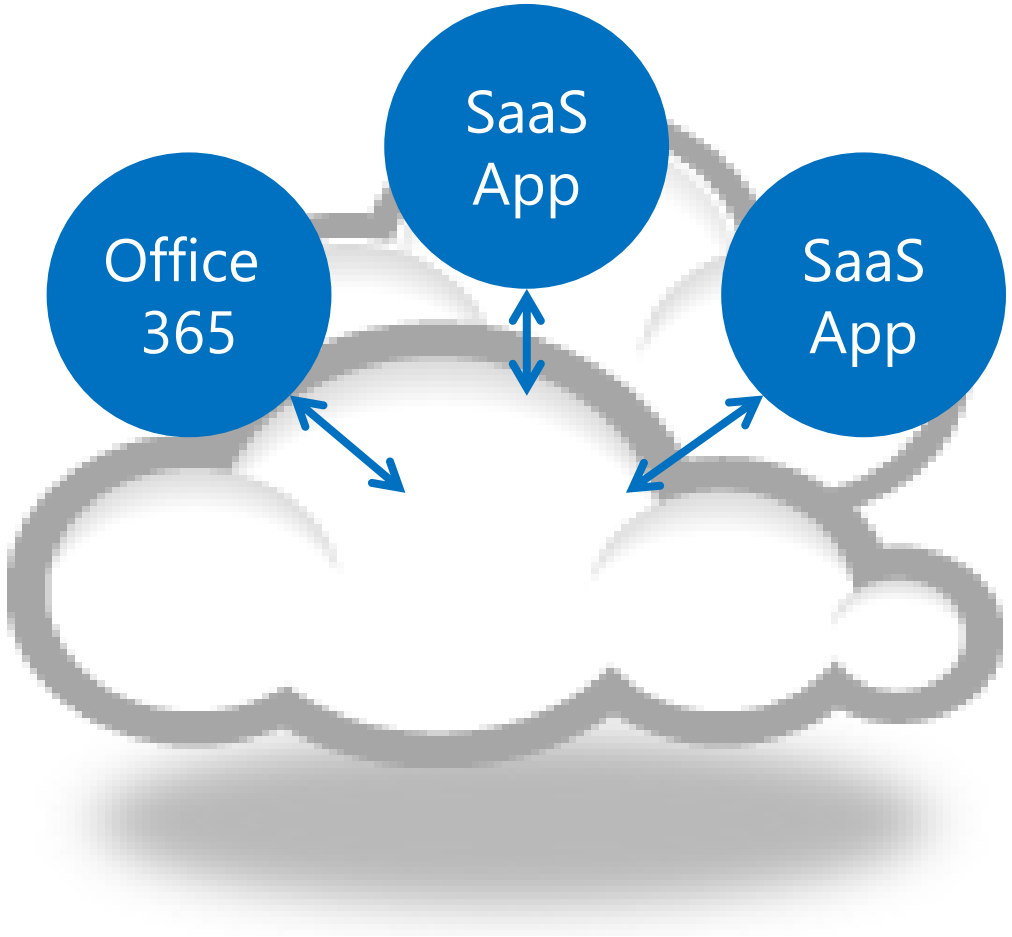
@maarten_goet

The challenge

Need to support cloud applications, for instance Office 365

Must run at Internet scale and be highly available

Support for Hybrid IT and existing Active Directory investment

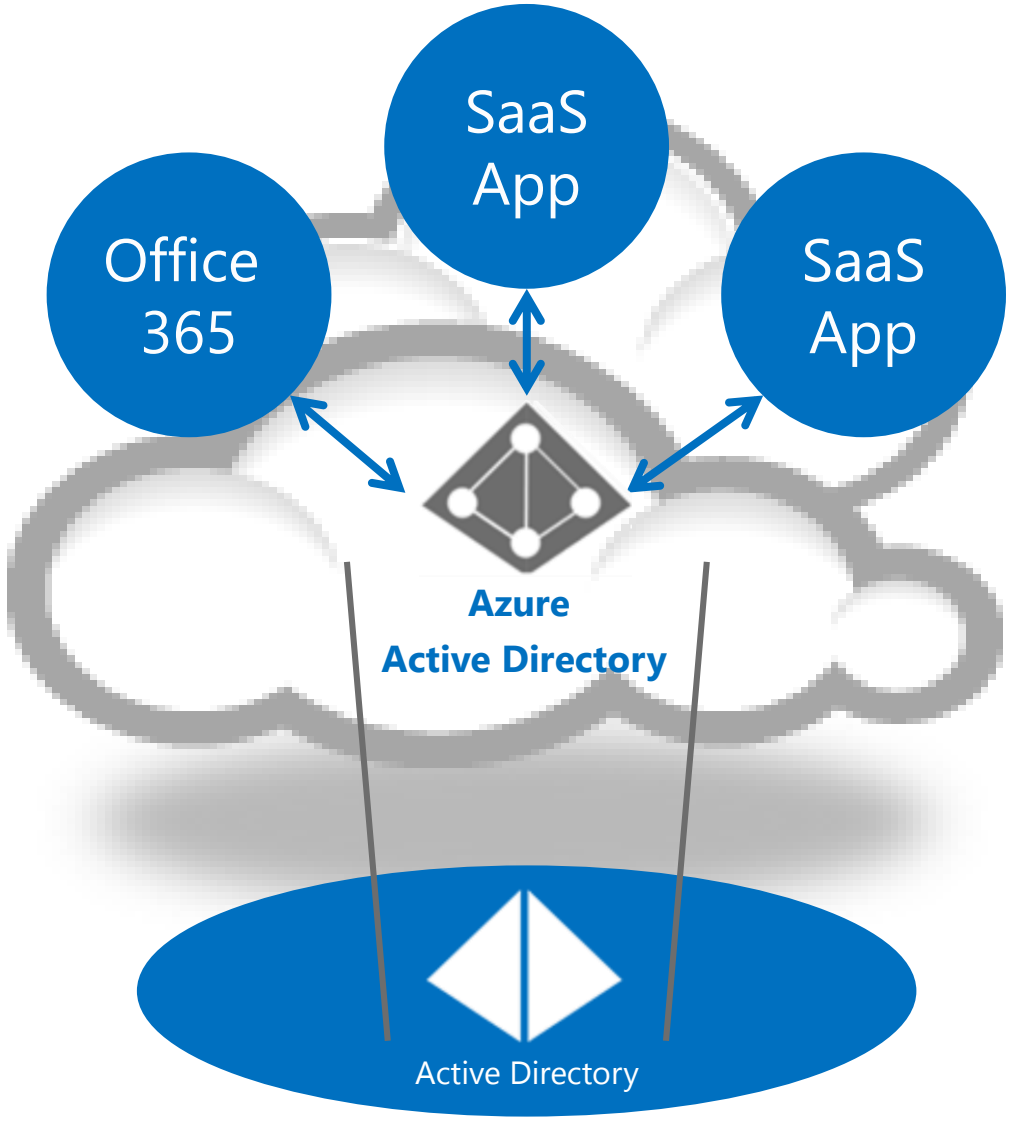


The solution – Windows Azure Active Directory

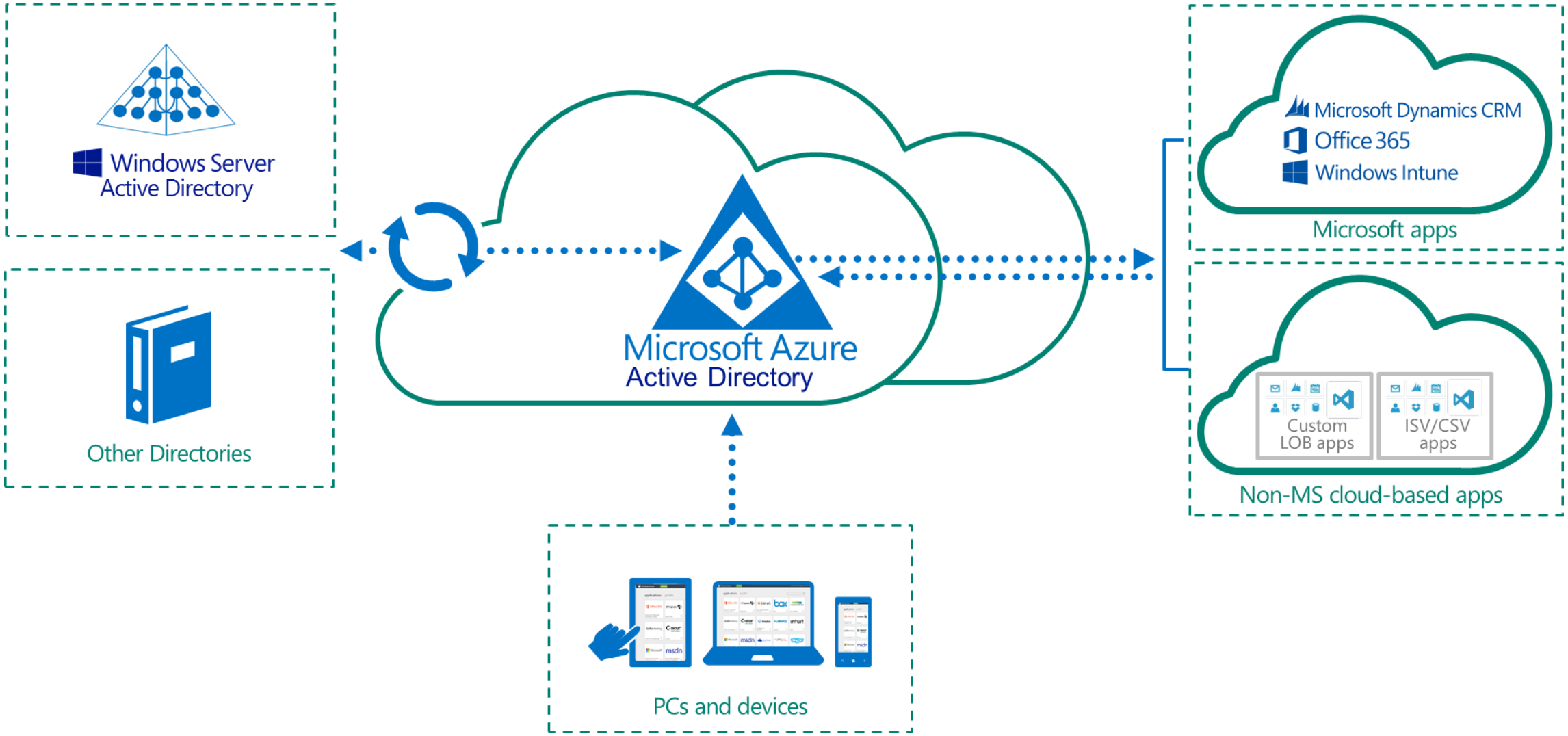
Active Directory revised to operate at Internet-scale multi-tenant directory service, built concurrently with Office 365

Extends Windows Server Active Directory into cloud

Provides cloud-based directory and identity services for organizations without Windows Server AD



Public identity as control point



Different editions

eatures	Azure AD (Free)	Azure AD Basic	AAD Premium
Directory as a Service	Up to 500k Objects	No Object Limit	No Object Limit
User/Group Management	Yes	Yes	Yes
SSO to pre-integrated SAAS Applications /Custom Apps	10 apps per user	10 apps per user	No Limit
Identity Synchronization Tool (WSAD Extension, Multi Forest, 3rd party)*	Yes	Yes	Yes
User-Based access management/provisioning	Yes	Yes	Yes
Self-Service Password Change for cloud users	Yes	Yes	Yes
Basic Security Reports	Yes	Yes	Yes
Cloud App Discovery (in public preview)	Yes	Yes	Yes
Group-based access management/provisioning		Yes	Yes
Self-Service Password Reset for cloud users		Yes	Yes
Company Branding (Logon Pages/Access Panel customization)		Yes	Yes
SLA		Yes	Yes
Identity Synchronization Tool advanced write-back capabilities (in preview)			Yes
Self-Service Group Management			Yes
Self-Service Password Reset/Change with on-premises write-back*			Yes
Advanced Security Reporting (machine learning-based)			Yes
Advanced Usage Reporting			Yes
MFA Cloud and On-premises (MFA Server)			Yes
IM CAL + FIM Server			Yes

Azure Active Directory Premium

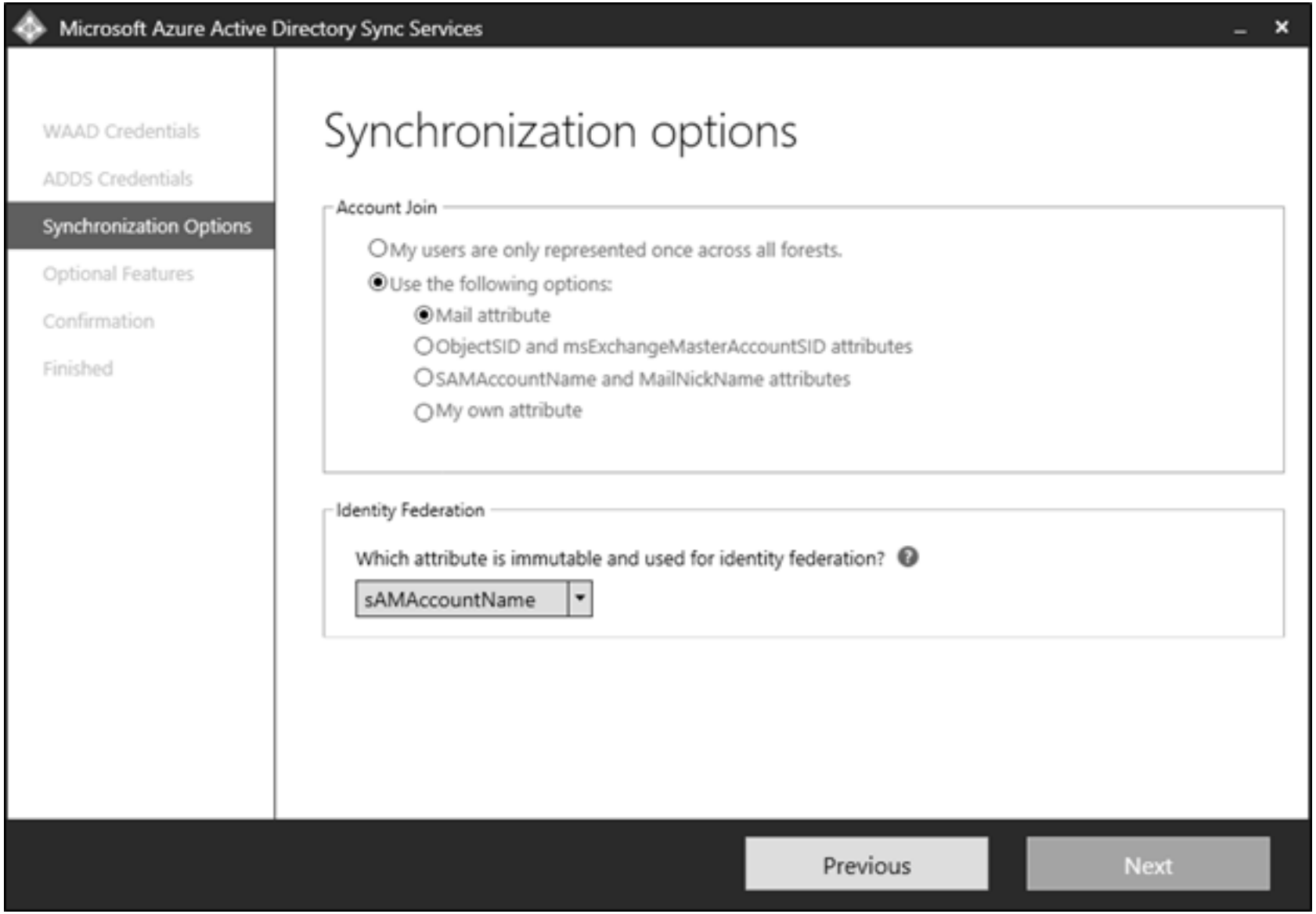
Built on top of the free offering, provides **a robust set** of capabilities to **empower enterprises** with demanding needs on identity and access management

Additionally, Azure AD premium offers:

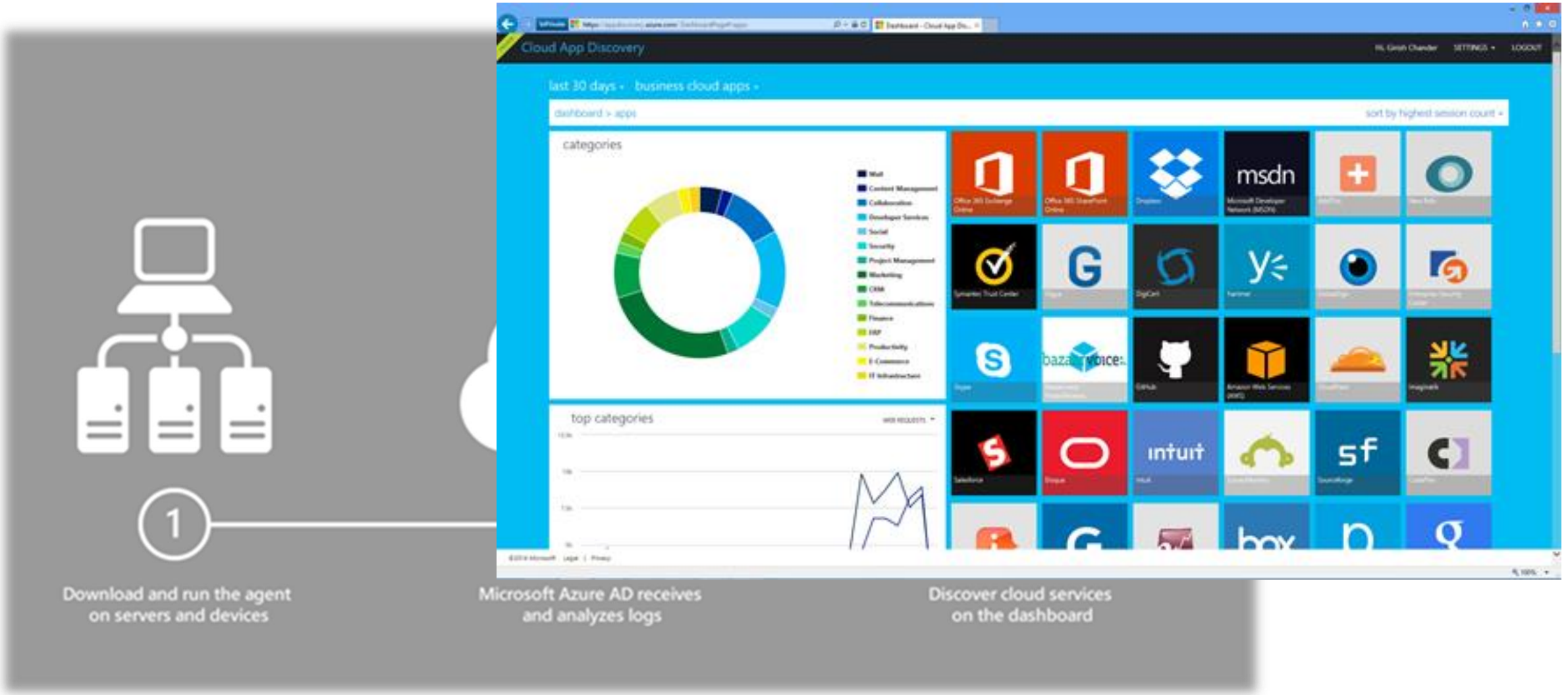
- An Enterprise SLA of **99.9%**

  Usage rights to **Forefront Identity Manager** Server and CALs

Azure Active Directory Sync Services Tool



Azure AD Cloud App Discovery Portal



Did you know?

There have been 900+ billion authentications through Windows Azure Active Directory worldwide.

That's nearly 120 authentications for every person on Earth!


DEMONSTRATION
Azure Active Directory

Multi-factor authentication

What is multi-factor?

AKA two-factor, 2FA, multi-factor, MFA, strong authentication

Any two or more of the following factors:

Something you know (a password or PIN)

Something you have (a phone, creditcard, or h/w token)

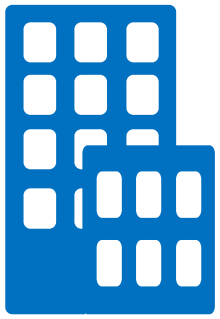
Something you are (a fingerprint, retinal scan, ..)

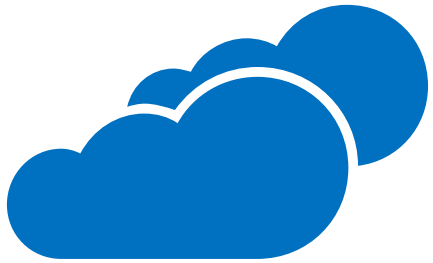
Stronger when using two different channels (out-of-band)

Azure Multi-Factor Authentication

r,
2012
f
to authenticate
employee, customer, and
partner access

Secures applications and
identities in the cloud and
on-premises





How it works

Mobile Apps

Push Notification

One-Time Passcode (OTP) Token

Phone Calls

Phone Call

Text Messages

Text Message

Azure MFA versus MFA for Office 365

	MFA for Office 365/Azure Administrators	Azure Multi-Factor Authentication
Administrators can Enable/Enforce MFA to end-users	✓	✓
Use Mobile app (online and OTP) as second authentication factor	✓	✓
Use Phone call as second authentication factor	✓	✓
Use SMS as second authentication factor	✓	✓
Application passwords for non-browser clients (e.g. Outlook, Lync)	✓	✓
Default Microsoft greetings during authentication phone calls	✓	✓
Custom greetings during authentication phone calls		✓
Fraud alert		✓
MFA SDK		✓
Security Reports		✓
MFA for on-premises applications/ MFA Server.		✓
One-Time Bypass		✓
Block/Unblock Users		✓
Customizable caller ID for authentication phone calls		✓
Event Confirmation		✓

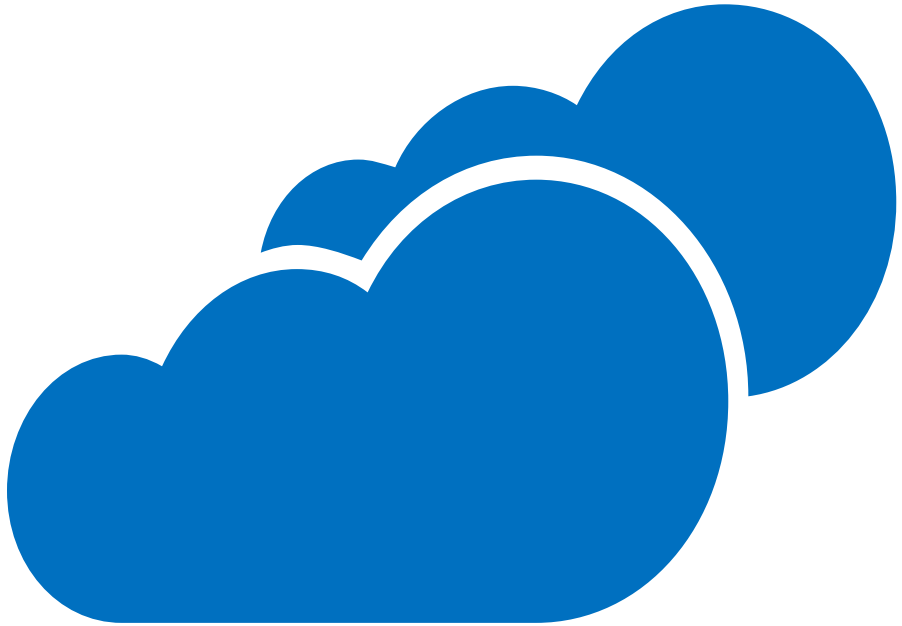

DEMONSTRATION
Multi-Factor Authentication

Summary

Active Directory revised to operate at Internet-scale multi-tenant directory service

Extends Windows Server Active Directory into cloud

Provides cloud-based directory and identity services for organizations without Windows Server AD




Thank you!
@maarten_goet