Microsoft

Azure Active Directory and Single Sign-On (SSO) with SAML 2.0 Identity Providers

Zion Brewer
Director Technical Business Development at Microsoft
linkedin.com/in/zionbrewer

John Gasper
IAM Consultant at Unicon, Inc.
linkedin.com/company/unicon-inc

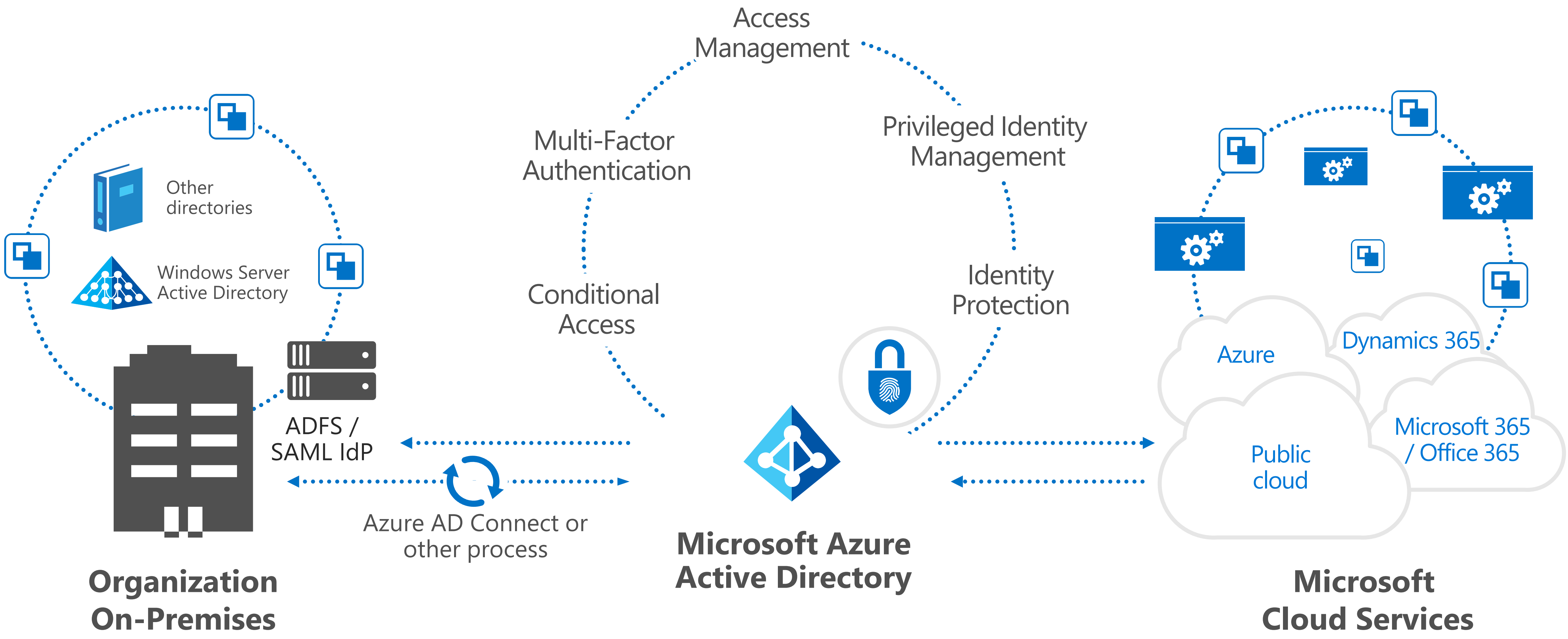
Azure AD and SSO with SAML 2.0 Identity Providers

Today's agenda

- What is Azure Active Directory?
- Why is Windows Server Active Directory required?
- How to get started with Azure AD and Office 365 Education
- Overview of single sign-on with SAML 2.0 identity providers
- Delegating authentication to Shibboleth IdP with John Gasper, IAM Consultant at Unicon, Inc.
- Next steps and additional resources available at https://aka.ms/Shibboleth

What is Azure Active Directory?

A trust fabric with security services for the Microsoft Cloud



Access Management
Multi-Factor Authentication
Privileged Identity Management
Conditional Access
Identity Protection
Other directories
Windows Server Active Directory
ADFS / SAML IdP
Azure AD Connect or other process
Organization On-Premises
Microsoft Azure Active Directory
Azure
Dynamics 365
Public cloud
Microsoft 365 / Office 365
Microsoft Cloud Services

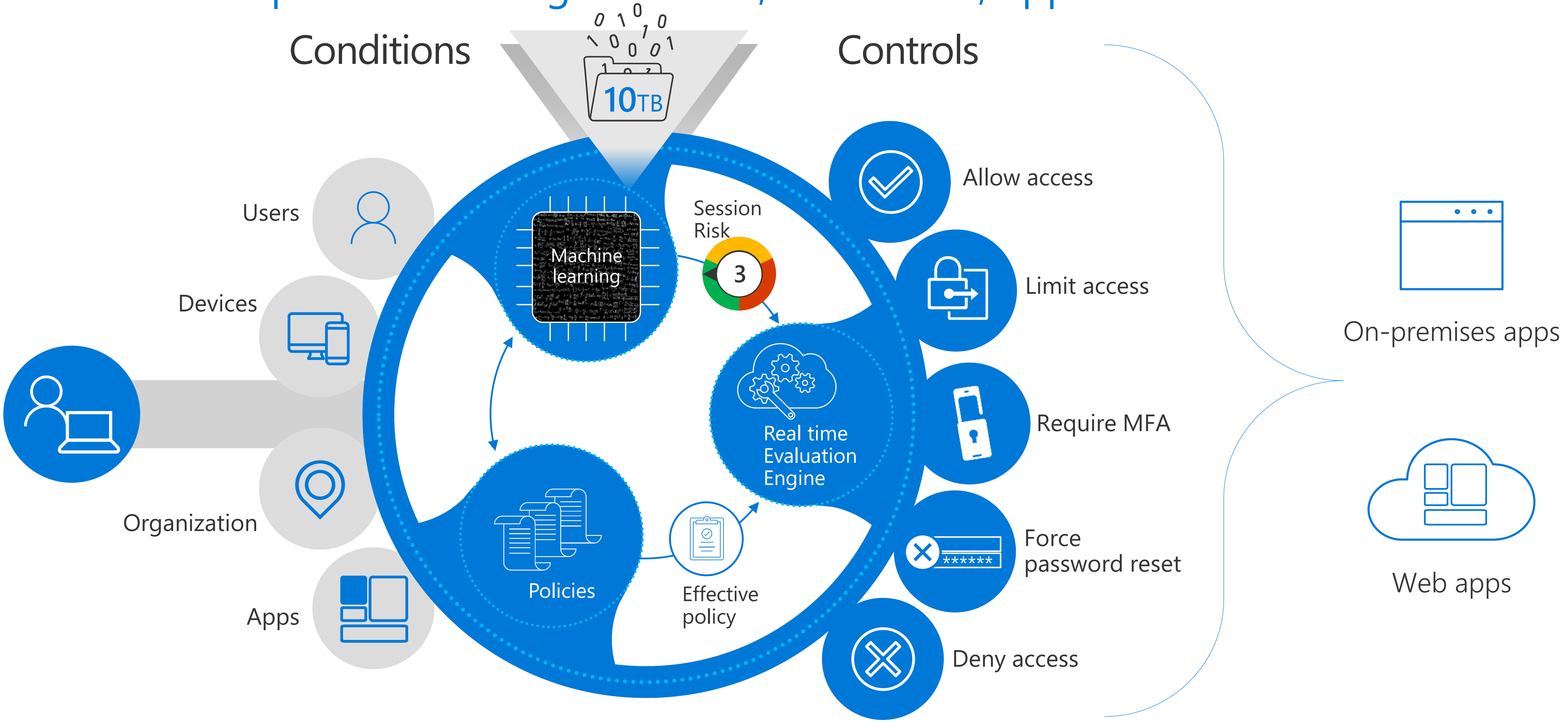
What is Azure Active Directory?

Identity and access management as a service

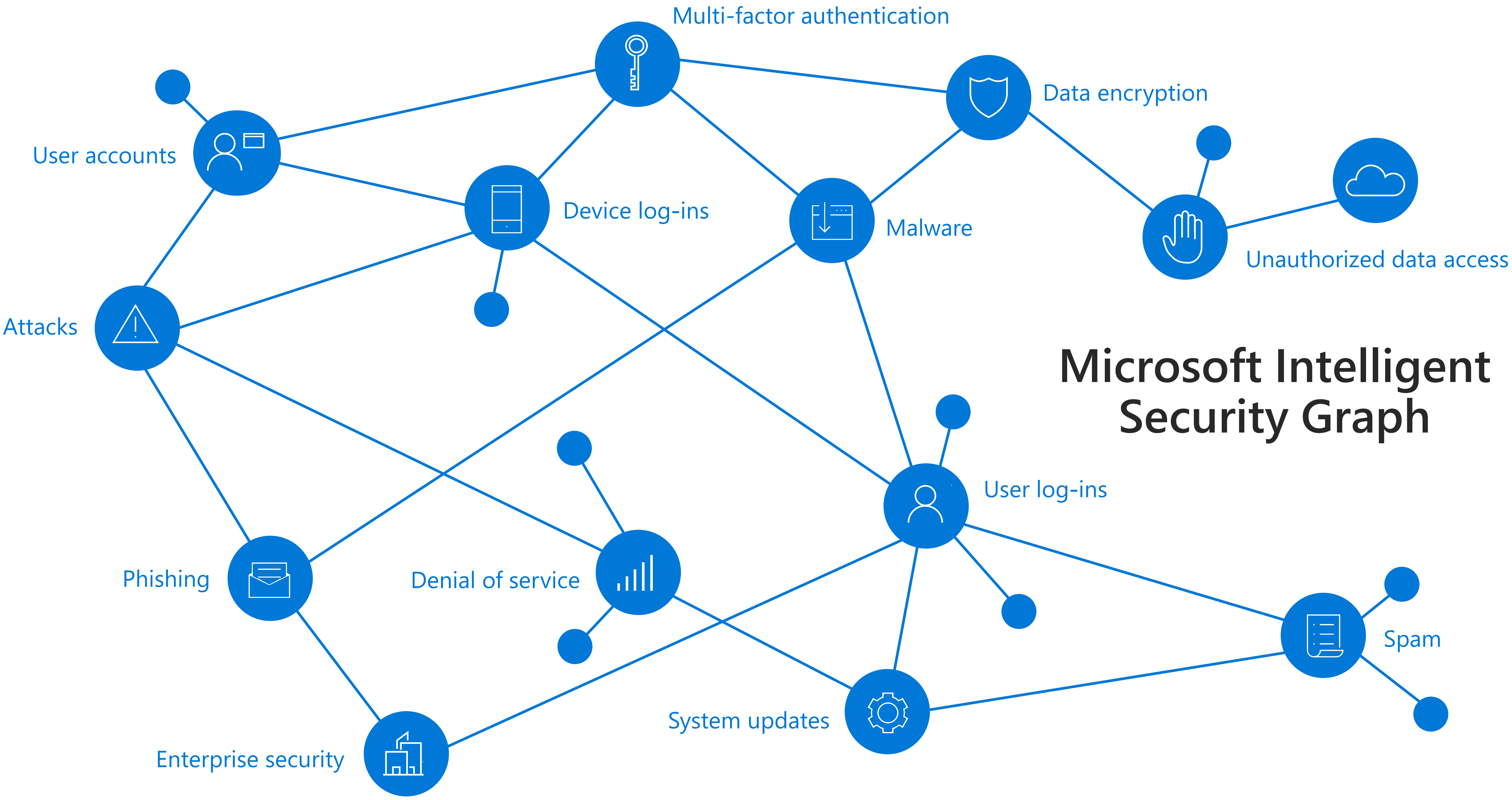
- B2B collaboration
- Provisioning-Deprovisioning
- Addition of custom cloud apps
- Access Panel/MyApps
- Dynamic Groups
- Identity Protection
- Self-Service capabilities
- Connect Health
- Remote Access to on-premises apps
- Azure AD B2C
- Group-Based Licensing
- Privileged Identity Management
- Azure AD Connect
- Conditional Access
- Microsoft Authenticator - Password-less Access
- Azure AD Join
- MDM-auto enrollment / Enterprise State Roaming
- Security Reporting
- SSO to SaaS
- Multi-Factor Authentication
- Azure AD DS
- Office 365 App Launcher
- HR App Integration
- Access Reviews

What is Azure Active Directory?

A multi-sided platform for organizations, individuals, apps and devices



Microsoft Intelligent Security Graph



Multi-factor authentication

Data encryption

User accounts

Device log-ins

Malware

Unauthorized data access

Attacks

User log-ins

Phishing

Denial of service

Spam

System updates

Enterprise security

Microsoft Graph

HTTPS://GRAPH.MICROSOFT.COM

Azure AD Excel Intune Outlook OneDrive OneNote SharePoint Planner

Single API that proxies multiple Microsoft services

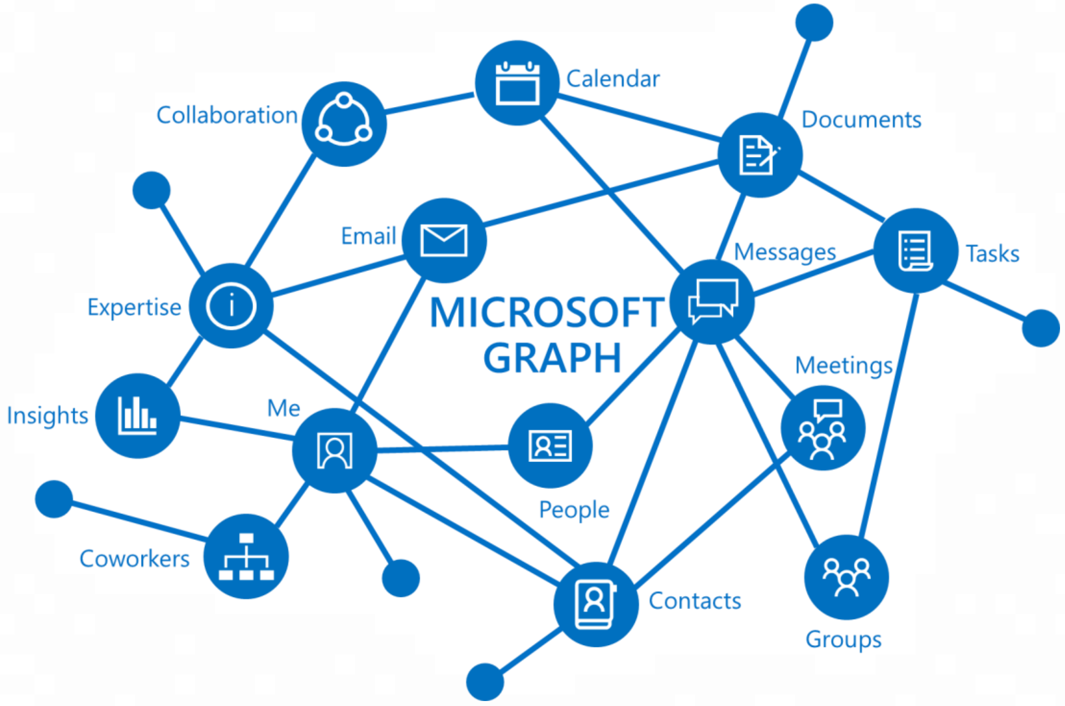
Allows for easy traversal of objects and relationships

Eliminates the need to discovery endpoints

Only one access token needed

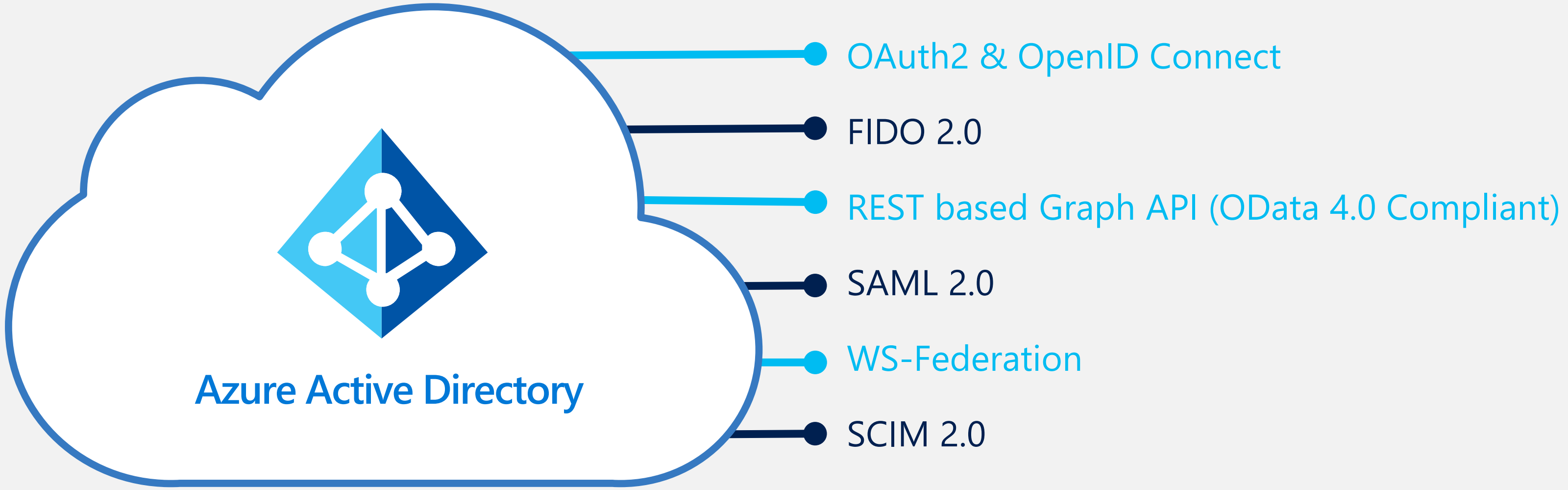
For both personal and work and school accounts

Exposing User data, Group data and Organizational data



Why is Windows Server Active Directory required?

It's NOT required! But Azure Active Directory is…



Azure Active Directory

- OAuth2 & OpenID Connect
- FIDO 2.0
- REST based Graph API (OData 4.0 Compliant)
- SAML 2.0
- WS-Federation
- SCIM 2.0

WS-Federation

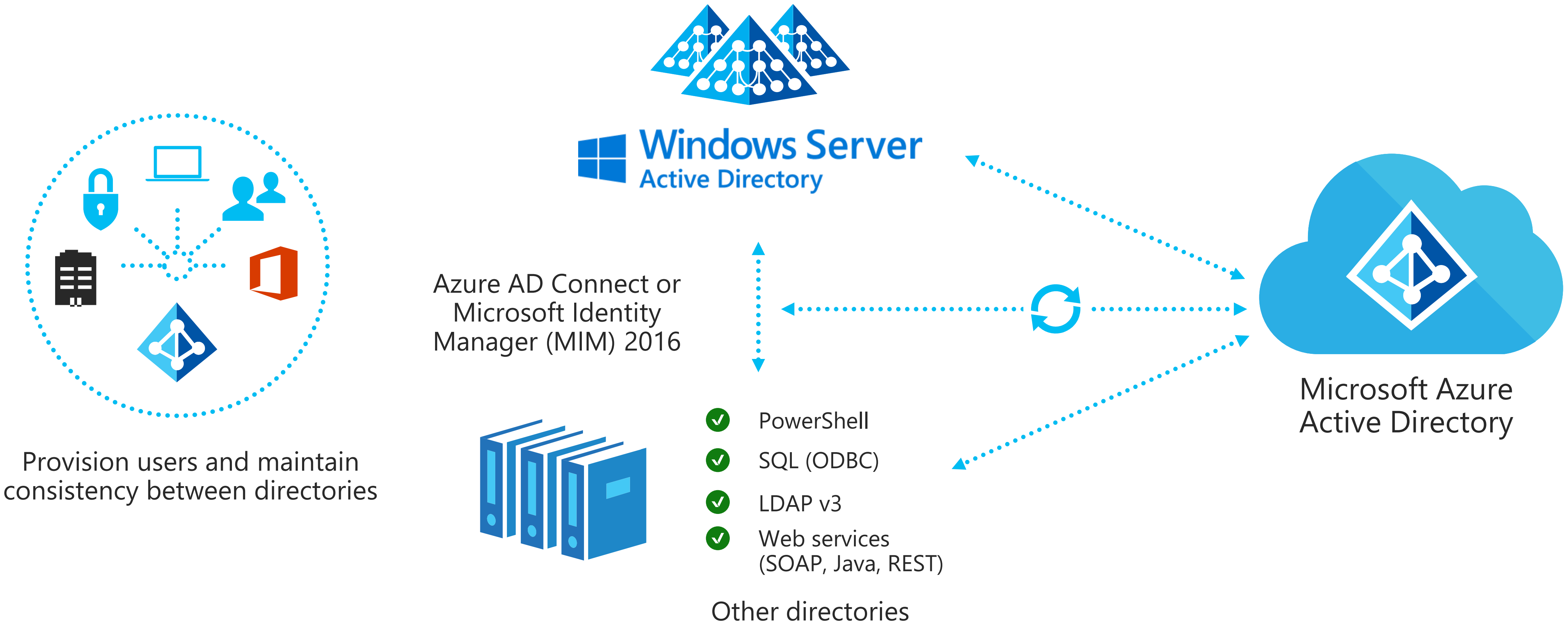
Strong support for modern, cross platform, cloud friendly API's & protocols

Certification program for third-party federation servers & services

Engaged with standards bodies OAuth, OpenID Connect, SCIM, SAML

Why is Windows Server Active Directory required?

It's NOT required! But there are considerations…

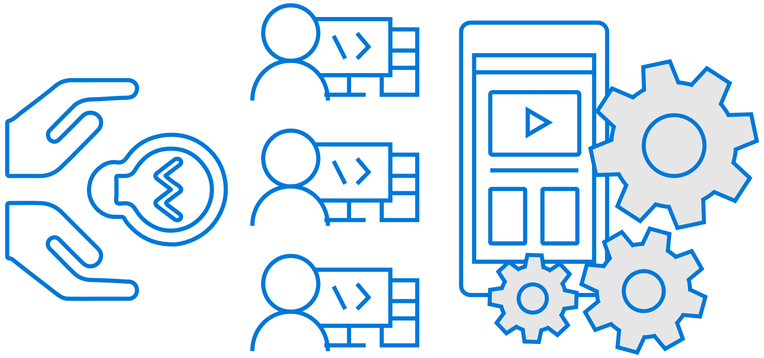


Provision users and maintain consistency between directories

- ✓ PowerShell
- ✓ SQL (ODBC)
- ✓ LDAP v3
- ✓ Web services (SOAP, Java, REST)

How to get started

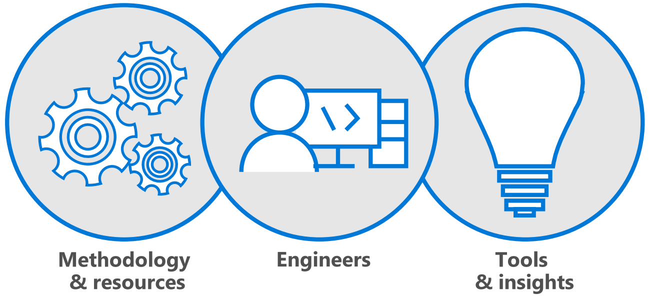
Try Azure Active Directory and Office 365 Education for free and use self-service resources



Let our team help with your implementation

FastTrack (https://fasttrack.microsoft.com)

Expert partners and Microsoft Engineering remote assistance to accelerate your Azure AD deployment



Get to production team

Microsoft Engineers engage directly to get you up and running with Azure Active Directory

Will Microsoft FastTrack help to configure a SAML 2.0 Identity Provider, e.g. Shibboleth IdP?

Overview of single sign-on with SAML 2.0 identity providers

General guidance for non-specific SAML 2.0 IdP deployment

- Sign up for Azure Active Directory or Office 365 Education
  - Add a custom domain name, e.g. test.contoso.edu
- Configure your SAML 2.0 identity provider
  - Add Azure AD metadata and configure Azure AD as a relying party
- Install Azure Active Directory Module for PowerShell
  - Use the MSOnline version on a Windows computer (for now)
- Set up a trust between your SAML 2.0 identity provider and Azure AD
  - Configure a domain for single sign-on and create a test account in that domain
- Verify Single Sign-On with your SAML 2.0 identity provider

Delegating Authentication to Shibboleth IdP

A Demo

About Unicon

EDUCATION TECHNOLOGY CONSULTING, SERVICES, & SUPPORT

Services, strategy, and support focused on the education industry

Deep domain-specific expertise

Open source software foundations

CLIENTS

Over 400 colleges and universities, several large publishers, and dozens of education technology companies

HISTORY

Founded in 1993 | Privately-held | Headquartered in Gilbert, AZ

Education Technology Domain Expertise

STUDENT SUCCESS

- Learning Analytics
- Visualizations and Dashboards
- Intervention Management

INTEGRATION

- Standards-based
- Custom Extensions
- Learning Ecosystem Delivery

LEARNING TECHNOLOGY

- Assessment – Formative, Summative
- Rich Content Creation & Delivery
- Learning Management

IDENTITY & ACCESS MANAGEMENT

- Web Single Sign-On
- Federated ID
- Groups Management

PORTALS

- Online Campus
- Community Development
- Collaboration

CLOUD SERVICES

- AWS Hosting
- Cloud Architecture
- Microservices

SERVICES | STRATEGY | SUPPORT

The Goal

- Delegate Office 365 user authentication to the Shibboleth IdP
  - Office 365 Web Applications & Azure Portal
  - Client apps supporting Office 365 Modern Authentication
- This demo only covers setting up Web SSO, and not ECP (i.e. ActiveSync, back-channel authentication)
- Shibboleth IdP v3.3.3 is being used, but older versions work as well

Prep Work

- Active Directory is already prepped with 2 accounts:
  - IdP User Search Account (Shib Service)
  - User account
- A new Office 365 tenant was just created, and the custom domain has been validated
- (Be sure to set the original domain back to “primary”)
- A DNS entry was setup in our custom domain for the IdP

Our Environment

- Microsoft Windows Server 2016
- Already downloaded and installed:
  - Java SE Development Kit 1.8
  - ~~Azure Active Directory module for Windows PowerShell~~
  - ~~Microsoft Online Services Sign-In Assistant~~
- Already downloaded:
  - Shibboleth IdP v3.3.3

Demo

1. Install and config Shibboleth IdP
2. Integrated Azure AD and Shibboleth IdP
3. Authenticate to Office 365
4. Authenticate to Azure Portal

Resources

- Companion Document:
  - http://aka.ms/Shibboleth
- Shibboleth Website:
  - http://www.shibboleth.net
- Need help?
  - http://www.unicon.net

Microsoft

Thank you!

What are organizations doing with Azure AD?

Benefits	Feature(s)
Reducing help desk costs	Self-Service Password Reset
Automated access management to SaaS Apps	SSO Outbound provisioning
Secure and compliant access to corporate apps	MFA, Conditional Access, Provisioning Identity Protection, PIM
Remote access management for on-premises apps	Azure AD App Proxy (Kerberos, SAML)
Collaborating with partners	Azure AD B2B – cross tenant collaboration
Connecting to consumers / citizens	Azure AD B2C
Enabling anywhere / anytime workstyle	Windows 10 Azure AD Join Enterprise State Roaming Auto-MDM enrollment
Monitoring health of Windows Server AD/ADFS	Azure AD Connect Health