

Azure Active Directory Premium

Andres Canello
Senior Program Manager
Azure Active Directory

The current reality



On-premises



Managed devices



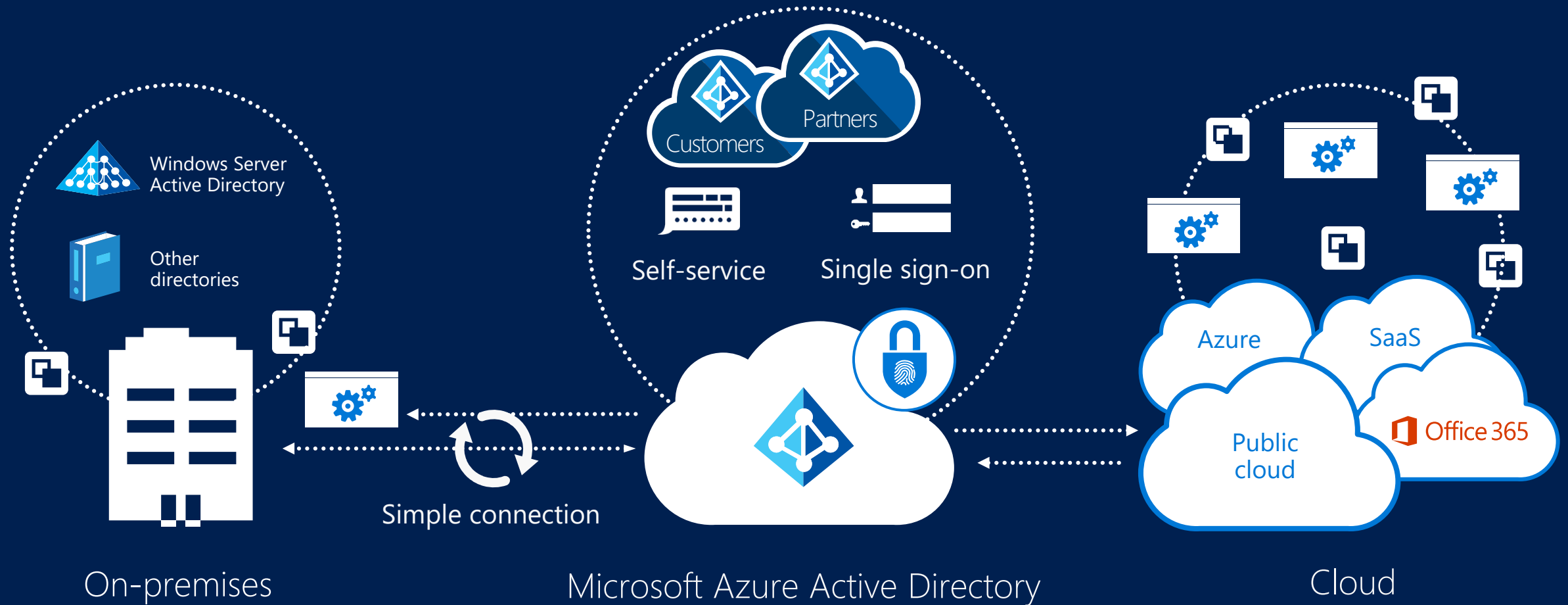
Active Directory



Windows Server

Identity as the core of enterprise mobility

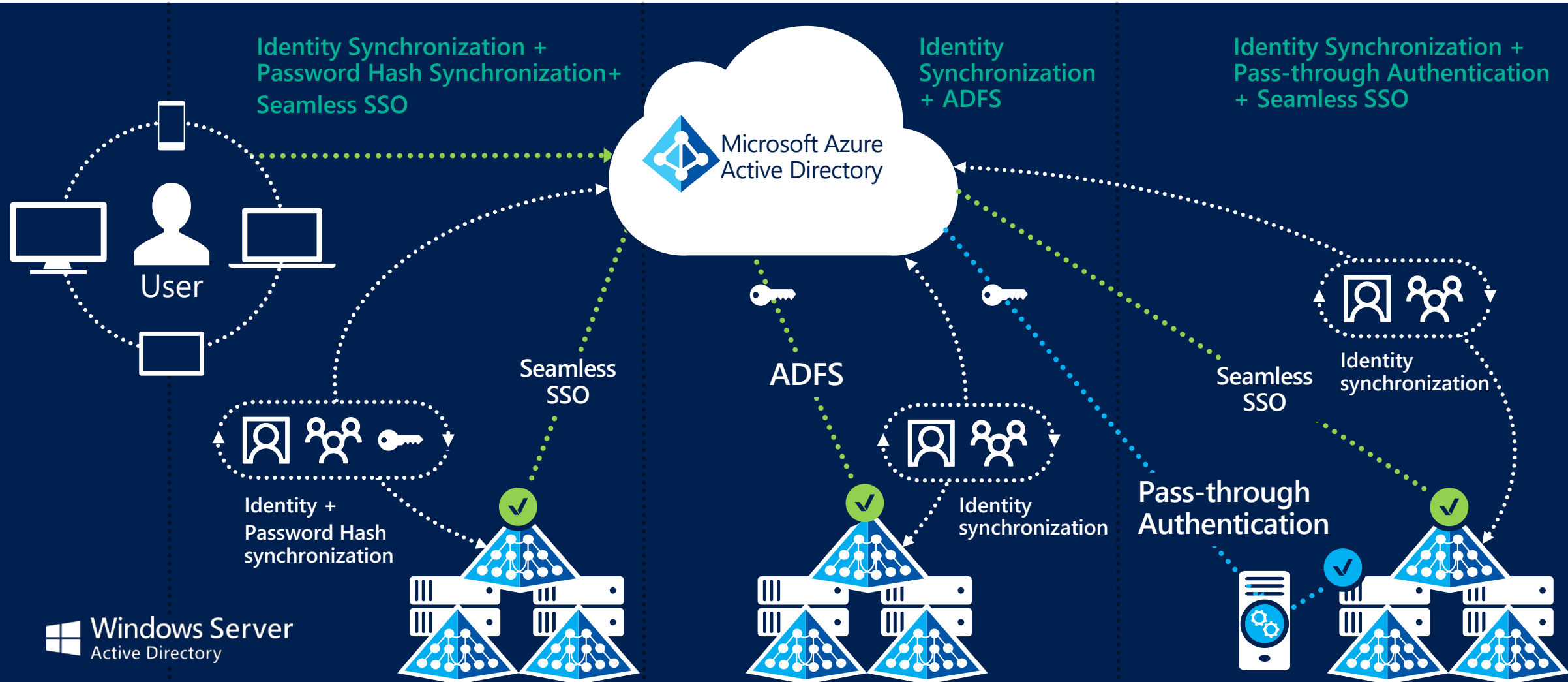
Azure Active Directory as the control plane



1000s OF APPS, 1 IDENTITY

Authentication with Azure Active Directory Connect

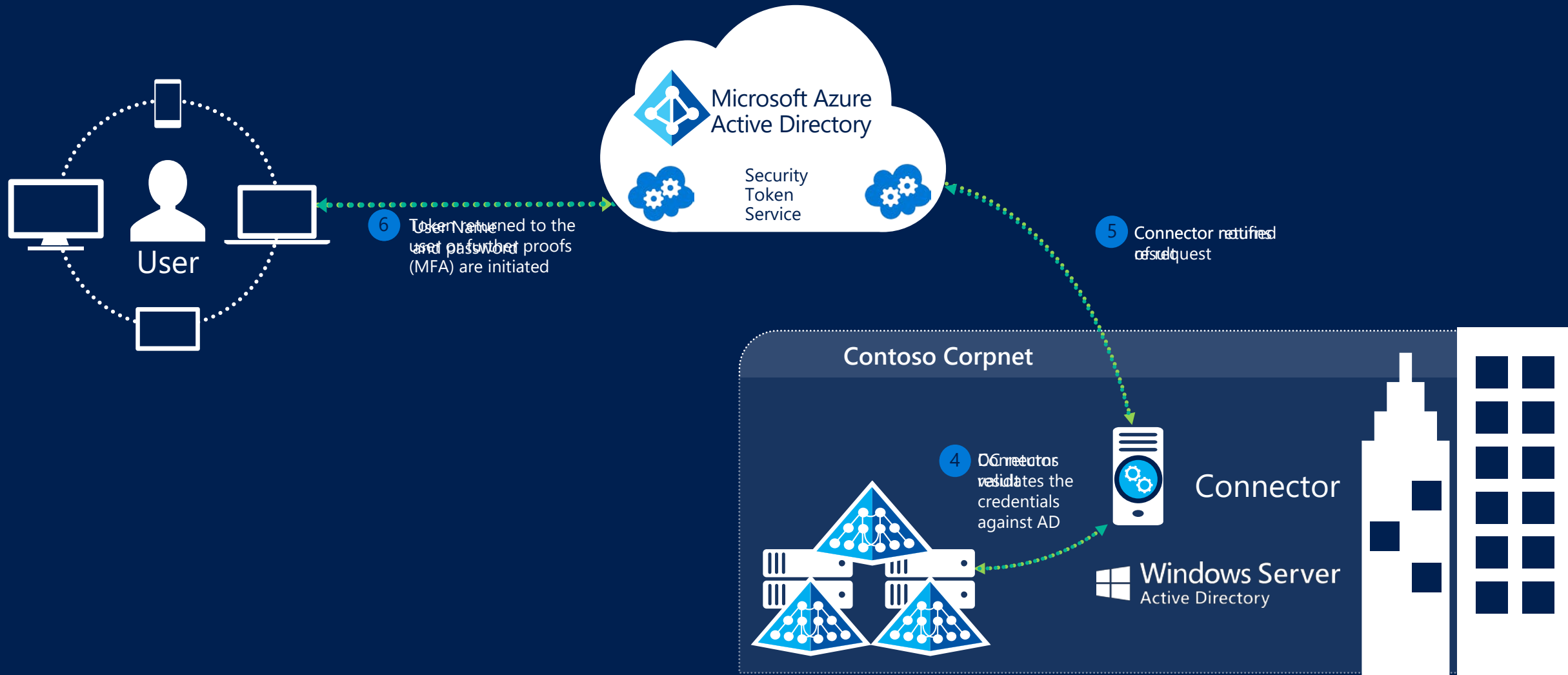
More options than ever!



1000s OF APPS, 1 IDENTITY

Azure Active Directory Pass-through authentication

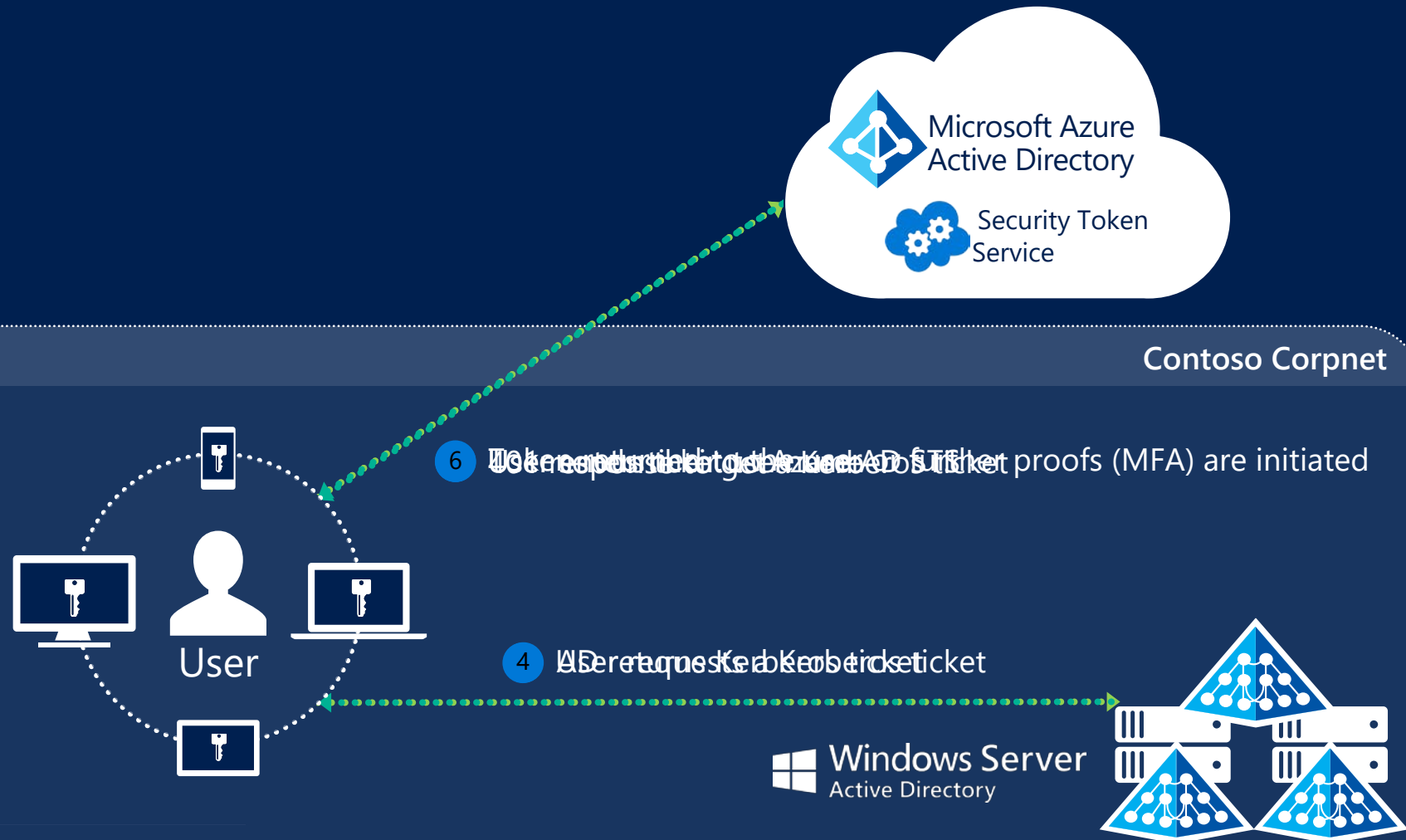
How it works

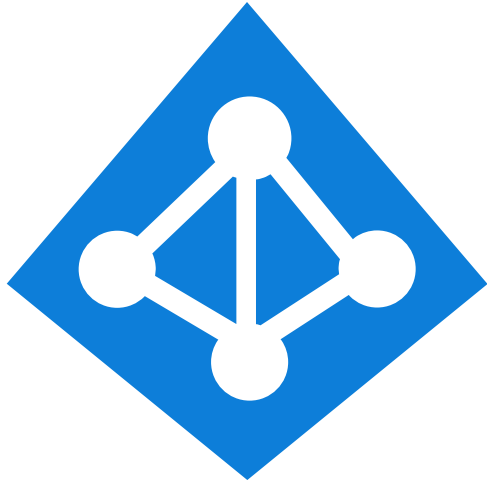


1000s OF APPS, 1 IDENTITY

Azure Active Directory

How seamless SSO works with Pass-through authentication and Password hash synchronisation



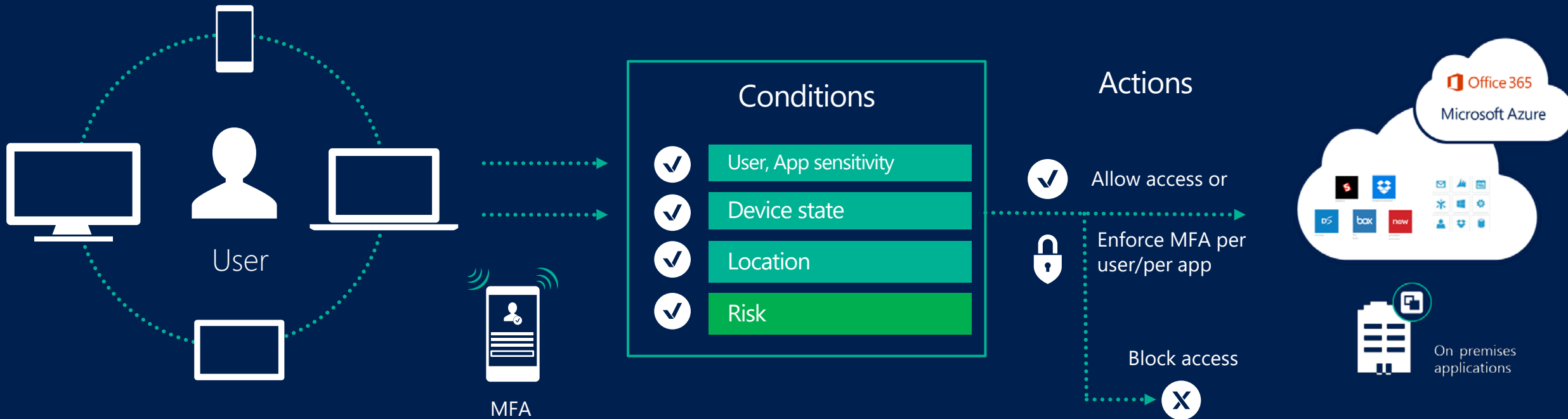


Azure Active Directory

 Azure AD Connect	 B2B collaboration	 Provisioning-Deprovisioning	 Conditional Access
 SSO to SaaS	 Self-Service capabilities	 Connect Health	 Multi-Factor Authentication
 Addition of custom cloud apps	 O365 Group Expiration	 Dynamic Groups	 Identity Protection
 Remote Access to on-premises apps	 Azure AD B2C	 Group-Based Licensing	 Privileged Identity Management
 Microsoft Authenticator - Password-less Access	 Azure AD Join	 MDM-auto enrollment / Enterprise State Roaming	 Security Reporting
 Azure AD DS	 Access Panel/MyApps	 HR App Integration	 Governance

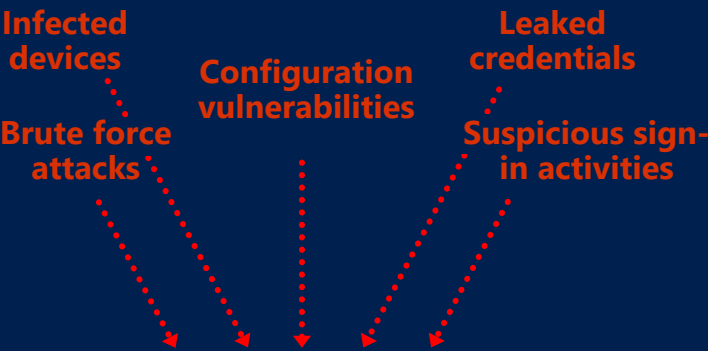
Conditional Access

Because "Who are you?" is not enough



Azure AD Reporting

Reporting

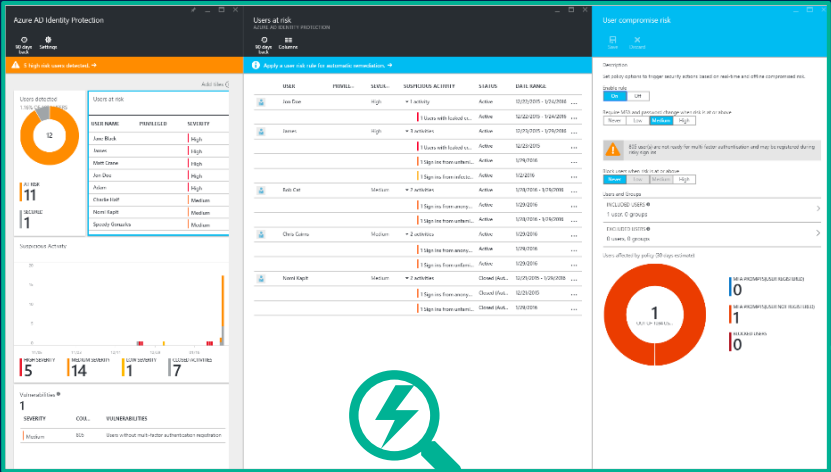


Activity

- Sign-in activities
- Audit logs

Security

- Risky sign-ins
- Users flagged for risk



Microsoft machine - learning engine

- Notifications
- Data Extracts/Downloads
- Reporting APIs

Reporting Solutions

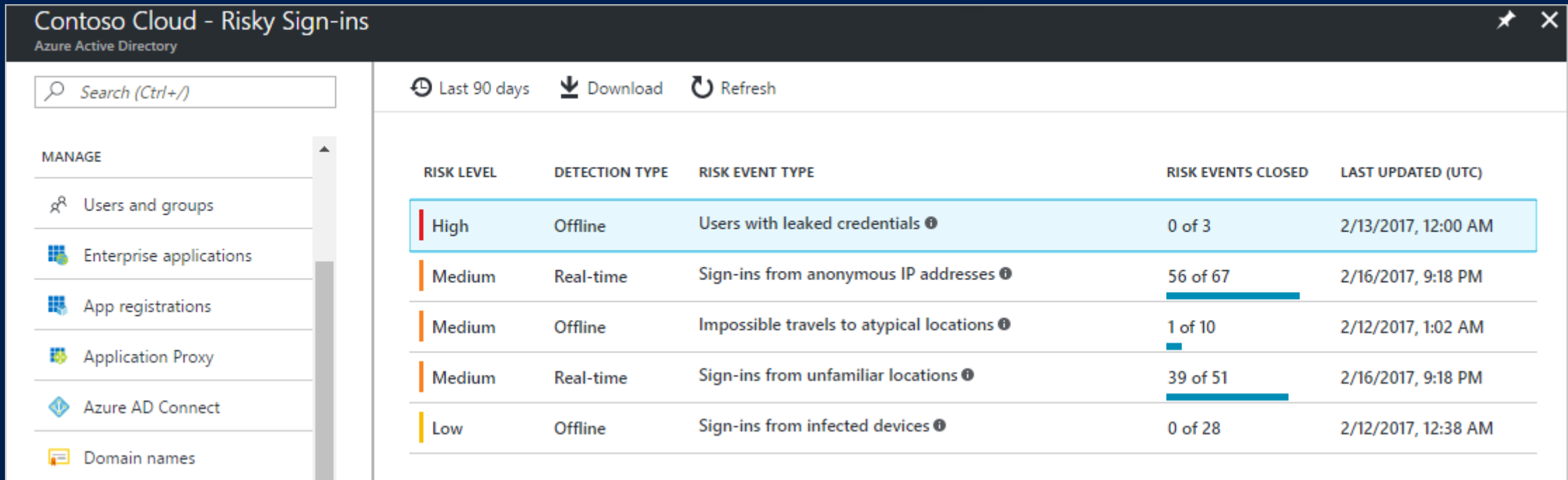


Apply Microsoft learnings to your existing security tools

Security Reports

Machine learning + secret sauce

- Azure AD Premium provides more reports and more data available to perform investigations



Contoso Cloud - Risky Sign-ins
Azure Active Directory

Search (Ctrl+/)

MANAGE

- Users and groups
- Enterprise applications
- App registrations
- Application Proxy
- Azure AD Connect
- Domain names

Last 90 days Download Refresh

RISK LEVEL	DETECTION TYPE	RISK EVENT TYPE	RISK EVENTS CLOSED	LAST UPDATED (UTC)
High	Offline	Users with leaked credentials ⓘ	0 of 3	2/13/2017, 12:00 AM
Medium	Real-time	Sign-ins from anonymous IP addresses ⓘ	56 of 67	2/16/2017, 9:18 PM
Medium	Offline	Impossible travels to atypical locations ⓘ	1 of 10	2/12/2017, 1:02 AM
Medium	Real-time	Sign-ins from unfamiliar locations ⓘ	39 of 51	2/16/2017, 9:18 PM
Low	Offline	Sign-ins from infected devices ⓘ	0 of 28	2/12/2017, 12:38 AM

Group-based licensing

Assigning licenses, the easy way

- Licenses can be assigned using any security group, cloud or synced from AD
- All Microsoft Online Services that require user-level licensing are supported
- Individual SKUs can be disabled, i.e.: Office 365 except Skype
- Dynamic Groups can be used, for example:
 - DG-O365-GBL: "CustomAttribute10 –contains 'O365'" -> O365E3 License
 - DG-EMS-GBL: "CustomAttribute10 –contains 'EMS'" -> EMSE3 License
 - User1: CustomAttribute10 = 'EMS;O365'

Office 365 Groups expiration

Spring cleaning time!

- Office 365 Groups
- grow and
- AADP

The screenshot shows the Microsoft Azure portal interface. On the left, the navigation pane includes 'Users and groups', 'Groups', 'Groups (beta)', 'Groups (beta) - Audit logs', 'Groups (beta) - Troubleshoot', and 'Groups (beta) - New support request'. The main pane displays the 'Expiration (preview)' settings for a group. A message from 'msonlineserviceteam@microsoftonline.com' states: 'Attention: Your Office 365 group has expired and been deleted. Restore it by 8/3/2017'. Below this, a red banner reads: 'Your Office 365 group 'Demo Office Group' has expired and been deleted on 7/5/2017'. A blue button labeled 'Restore group' is visible. At the bottom, a warning icon and text state: 'The group will only be restorable until 8/3/2017'. The footer of the message window shows 'Microsoft Corporation, One Microsoft Way, Redmond WA, 98052 | Privacy Statement'.

Members can

Connect Health: Monitor your Identity Bridge

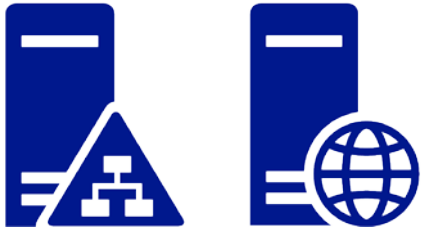
Monitor and gain insights into the identity infrastructure used to extend on-premises identities to Azure Active Directory and Office 365.

Monitor:

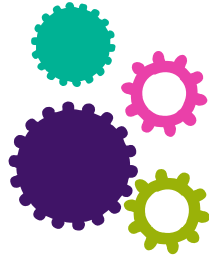
- The Azure AD Connect sync engine health
- ADFS infrastructure health
- On-premises AD Domain Services health



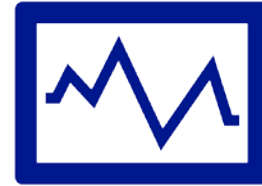
Investigating without Connect Health



Access all AD
FS and WAP
server



Check service
is ok on each
server



Check for any
stress signals
on servers



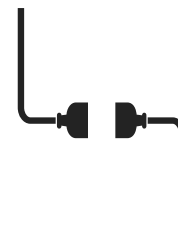
Check audit
events on all
servers



Check if
tokens are
being issued

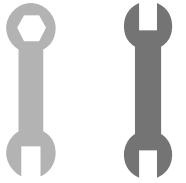


Check connect
server for sync
issues



Check external
connectivity
issues

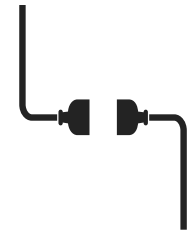
Investigating with Connect Health



Check Connect
Health for
AD FS

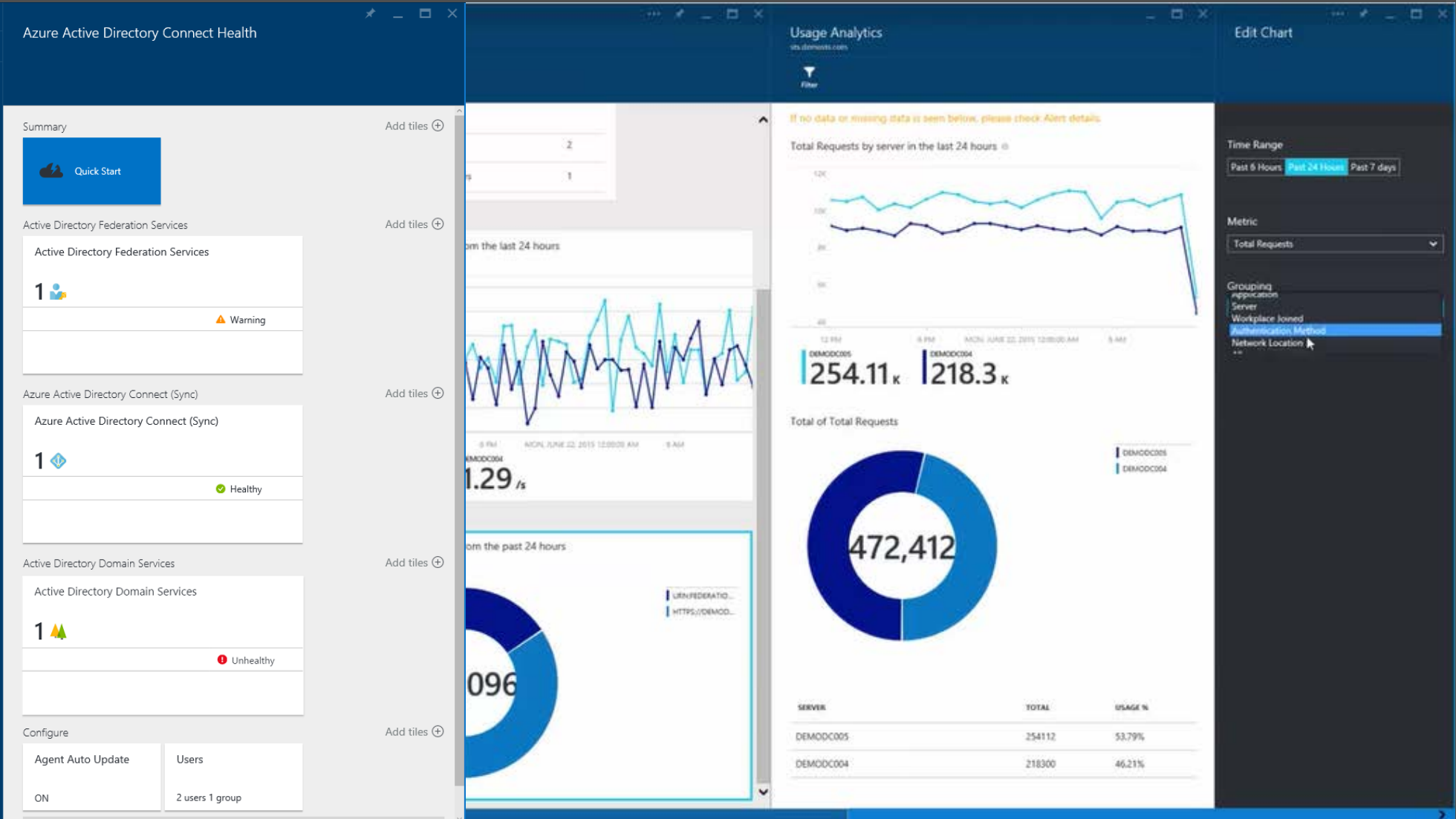


Check Connect
Health for
Sync



Check external
connectivity
issues

Azure Active Directory Connect Health Portal





Thanks!