#ExpertsLiveNO

Experts Live Norway

Why you should Cloud Attach your ConfigMgr and Windows 10 environment

Marius A. Skovli

CTGlobal Principal Consultant
Microsoft Enterprise Mobility MVP
@MariusSkovli

Platinum Sponsor 2019

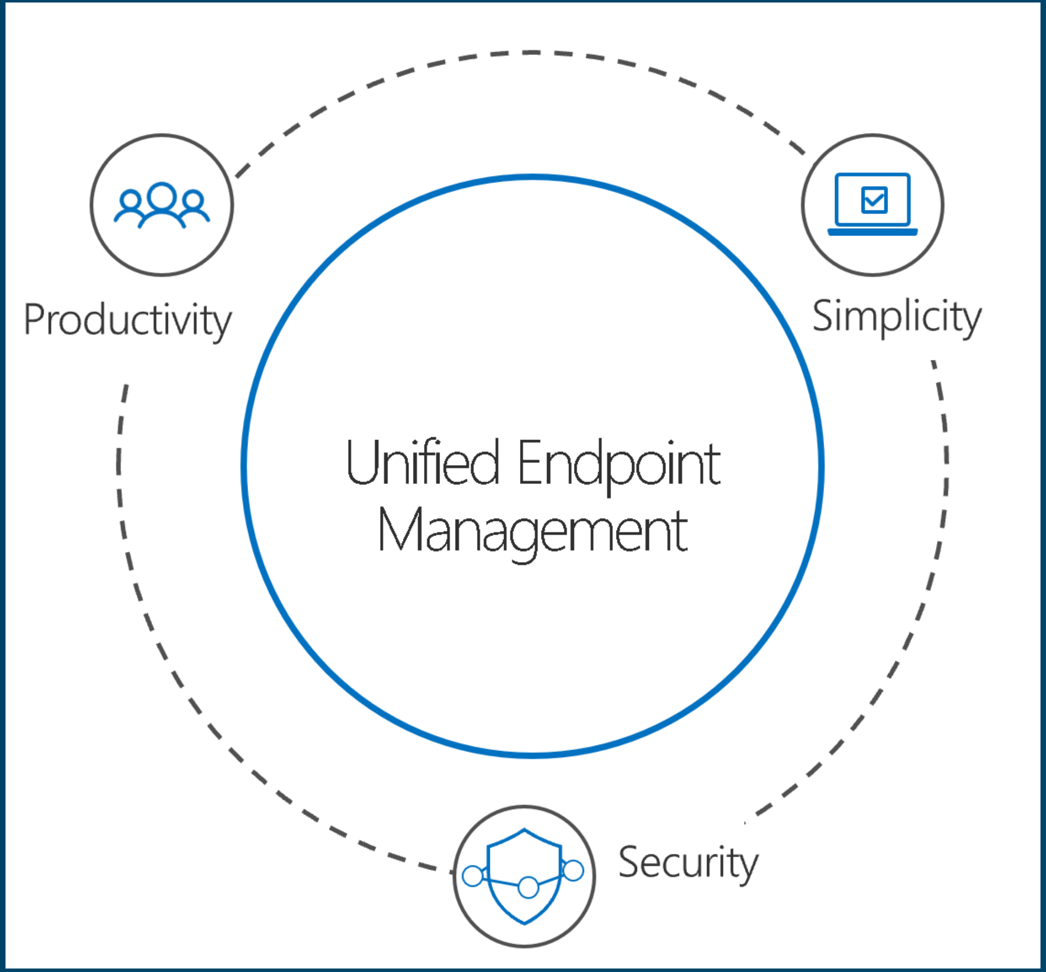
Microsoft

Agenda

- Learn why you should cloud-attach
- Learn about the benefits about connecting ConfigMgr to Azure.
- In this session we will dive into what it takes and why you should extend SCCM to the cloud!
- Where does Intune fit into the picture?
- What about Conditional Access and Remote actions?
- Learn how this will improve user experience in Windows 10

Questions?

Now, why should you cloud-attach?



Now, why should you cloud-attach?

Harness cloud capabilities without causing to much stress and friction in your organization!

Now, why should you cloud-attach?

	On-premises	Cloud attached	Cloud only
Traditional OS Deployment	✓	✓	
Win32 app management	✓	✓	✓
Configuration and GPO	✓	✓	✓
Bitlocker Management	✓	✓	✓
Hardware and software inventory	✓	✓	✓
Update management	✓	✓	✓
Unified Endpoint Management – Windows, iOS, macOS, Android		✓	✓
Modern access control – Compliance, Conditional Access		✓	✓
Modern provisioning – Autopilot, DEP, Zero Touch, KME		✓	✓
Modern security – Hello, Attestation, ATP, Secure Score		✓	✓
Modern policy – Security Baselines, Guided Deployments		✓	✓
Modern app management – O365 Pro Plus, Stores, SaaS, VPP		✓	✓
Full M365 integration – Analytics, Graph, Console, RBAC, Audit		✓	✓

Now, why should you cloud-attach?

- Conditional access with device compliance!!
- Centralized visibility of device health
- Modern provisioning with Windows Autopilot!!
- Remote actions
- *ConfigMgr Application deployment*
- *ConfigMgr Advanced Inventory*
- *ConfigMgr CMPivot*

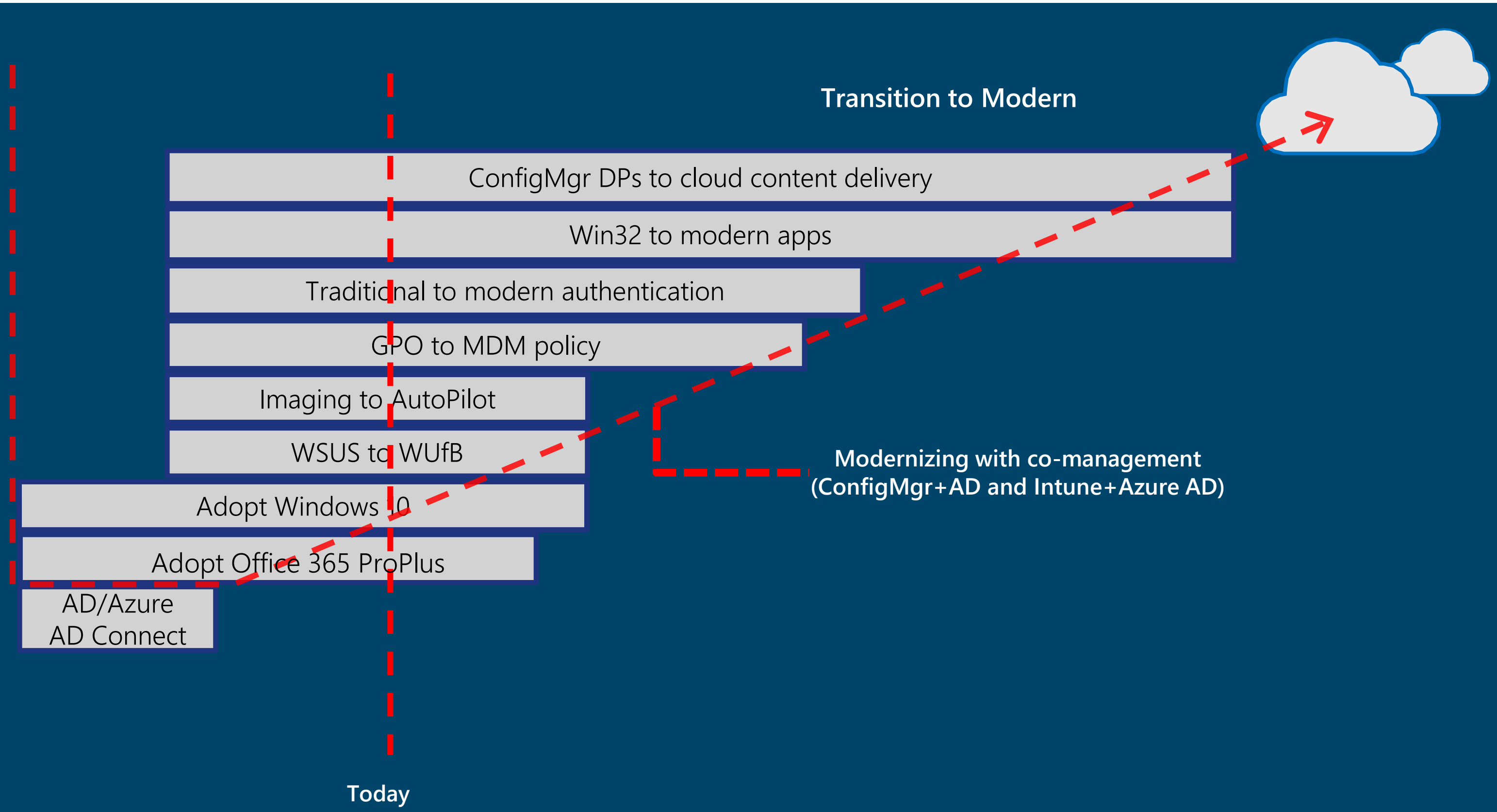
(Quick Demo)

- ConfigMgr CMPivot
  - On Azure AD Only Device
  - On Hybrid AAD Device

The message from Microsoft

On-premises		Modern Workplace
Legacy devices	→	Modern devices
Windows 7	→	Windows 10
Office	→	Office 365
Active Directory	+	Azure Active Directory
ConfigMgr	+	Microsoft Intune
Windows Defender	+	Microsoft Threat Protection

Transitioning to modern management



Transition to Modern

ConfigMgr DPs to cloud content delivery

Win32 to modern apps

Traditional to modern authentication

GPO to MDM policy

Imaging to AutoPilot

WSUS to WUfB

Adopt Windows 10

Adopt Office 365 ProPlus

AD/Azure
AD Connect

Modernizing with co-management
(ConfigMgr+AD and Intune+Azure AD)

Today

Existing Configuration Manager clients (domain joined devise):

You have Windows 10 devices that are already managed by ConfigMgr. You set up hybrid Azure AD, and enroll them into Intune.

New internet-based devices (Azure AD + Intune managed devices):

You have new Windows 10 devices that join Azure AD and automatically enroll to Intune. You install the Configuration Manager client to reach a co-management state.

Getting Ready for Cloud Attach

Licensing

Azure AD Premium
EMS/Intune

Configuration Manager

1710 or later

Azure Active Directory Premium

MDM Autoenrollment enabled

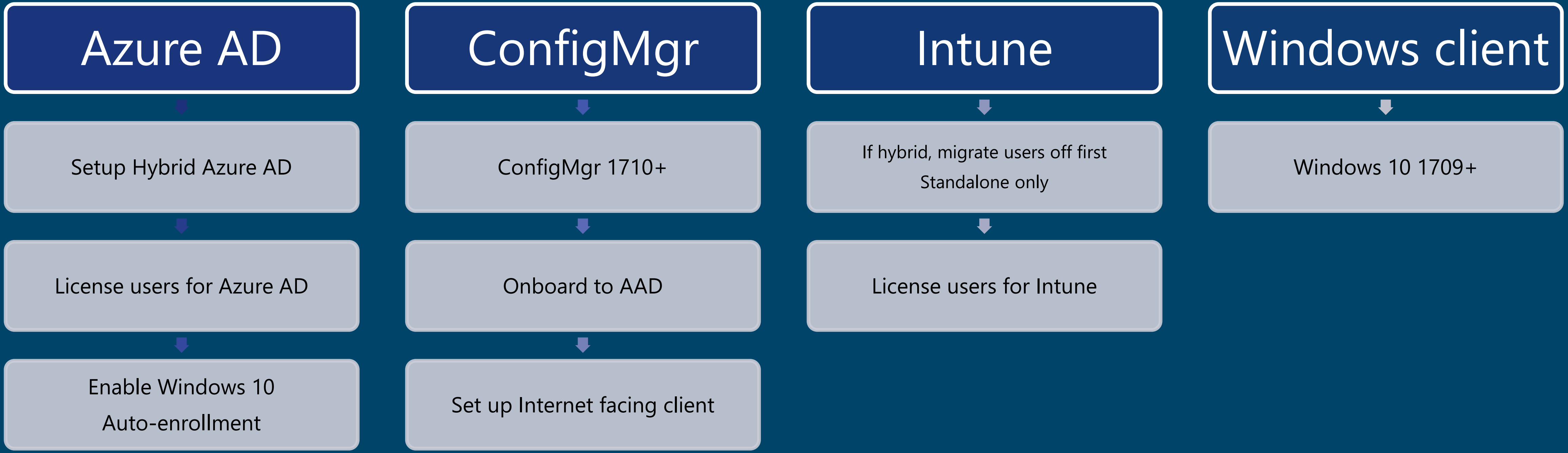
Microsoft Intune

MDM Authority set to Intune

Windows 10

1709 or later

Getting Ready for Cloud Attach



Azure AD

- Setup Hybrid Azure AD
- License users for Azure AD
- Enable Windows 10 Auto-enrollment

ConfigMgr

- ConfigMgr 1710+
- Onboard to AAD
- Set up Internet facing client

Intune

- If hybrid, migrate users off first
Standalone only
- License users for Intune

Windows client

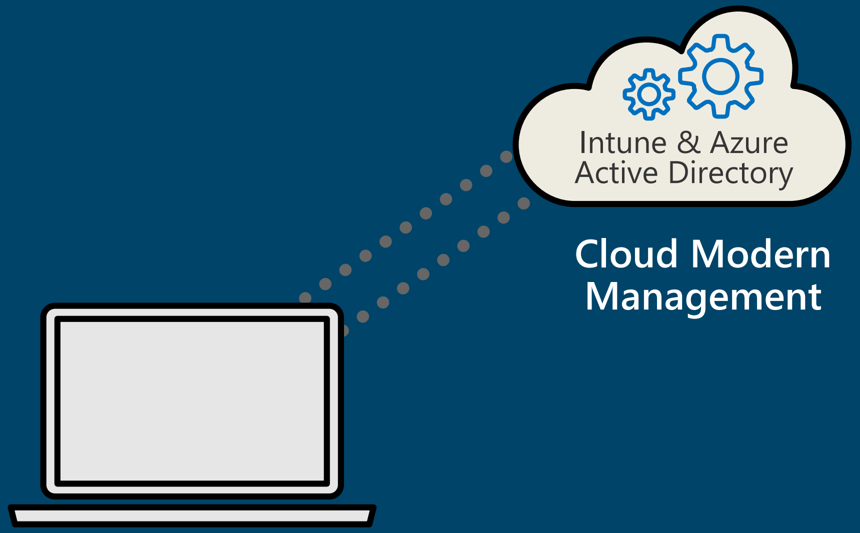
- Windows 10 1709+

Getting Ready for Cloud Attach

- Prerequisites (Domain joined devices)
  - Hybrid Azure AD Join
  - Windows 10 Devices joined to both AD and AAD
  - (Cloud Management Gateway)

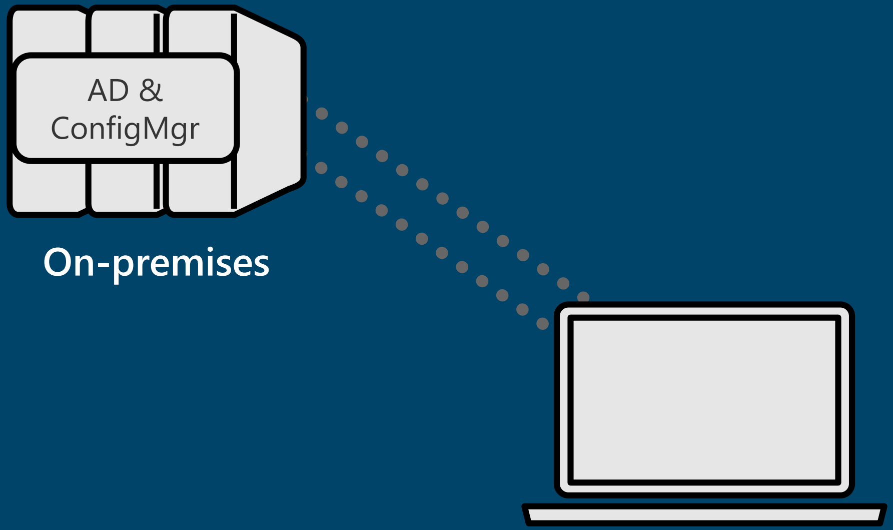
- Prerequisites (Azure AD joined devices)
  - Cloud Management Gateway

Management architectures: Cloud only

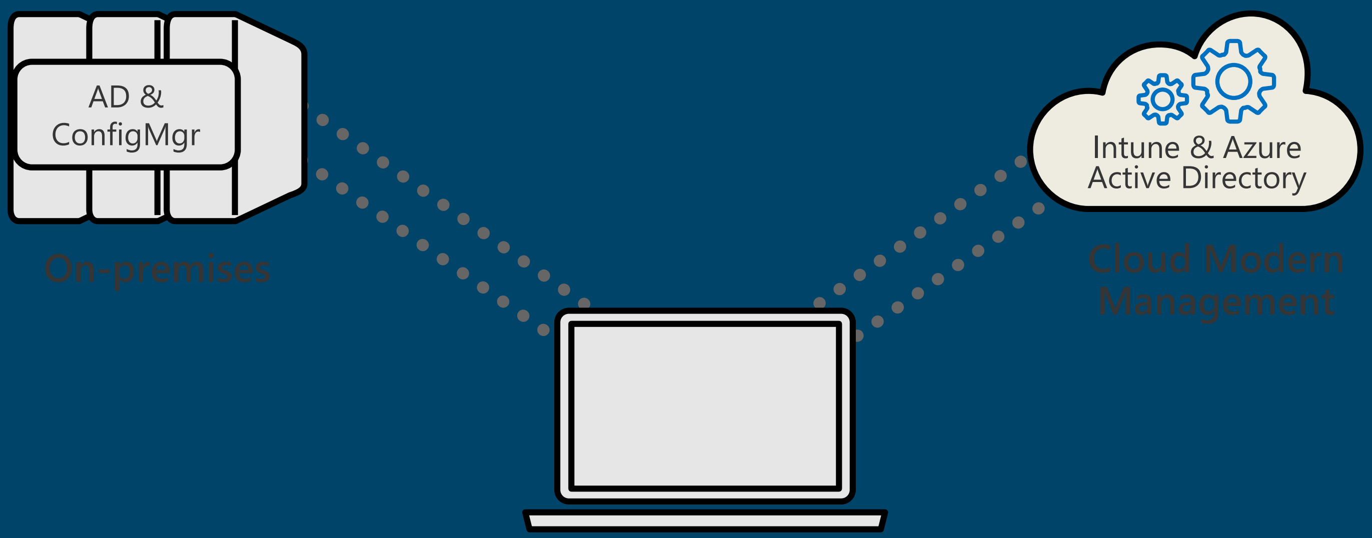


Cloud Modern Management

Management architectures: On-prem only

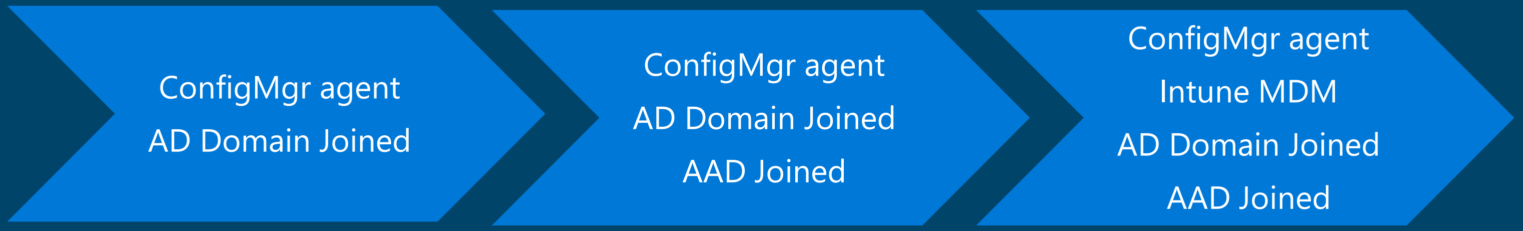


Management architectures: Co-managed



How to get to co-management

Existing ConfigMgr managed devices

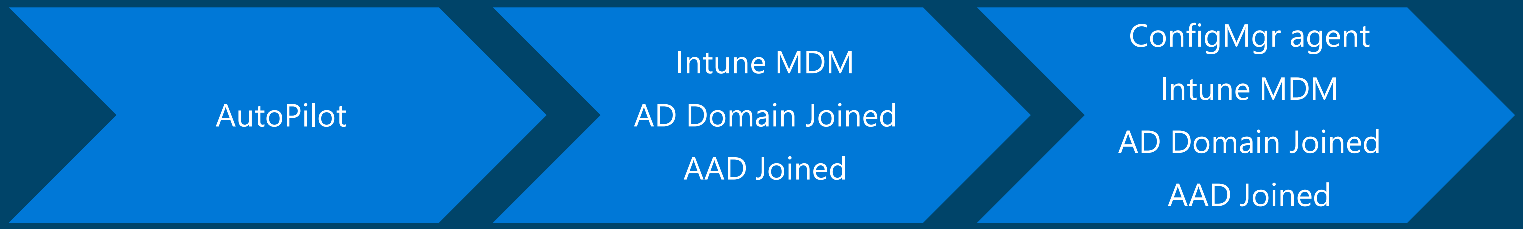


ConfigMgr agent
AD Domain Joined

ConfigMgr agent
AD Domain Joined
AAD Joined

ConfigMgr agent
Intune MDM
AD Domain Joined
AAD Joined

Modern Provisioning



AutoPilot

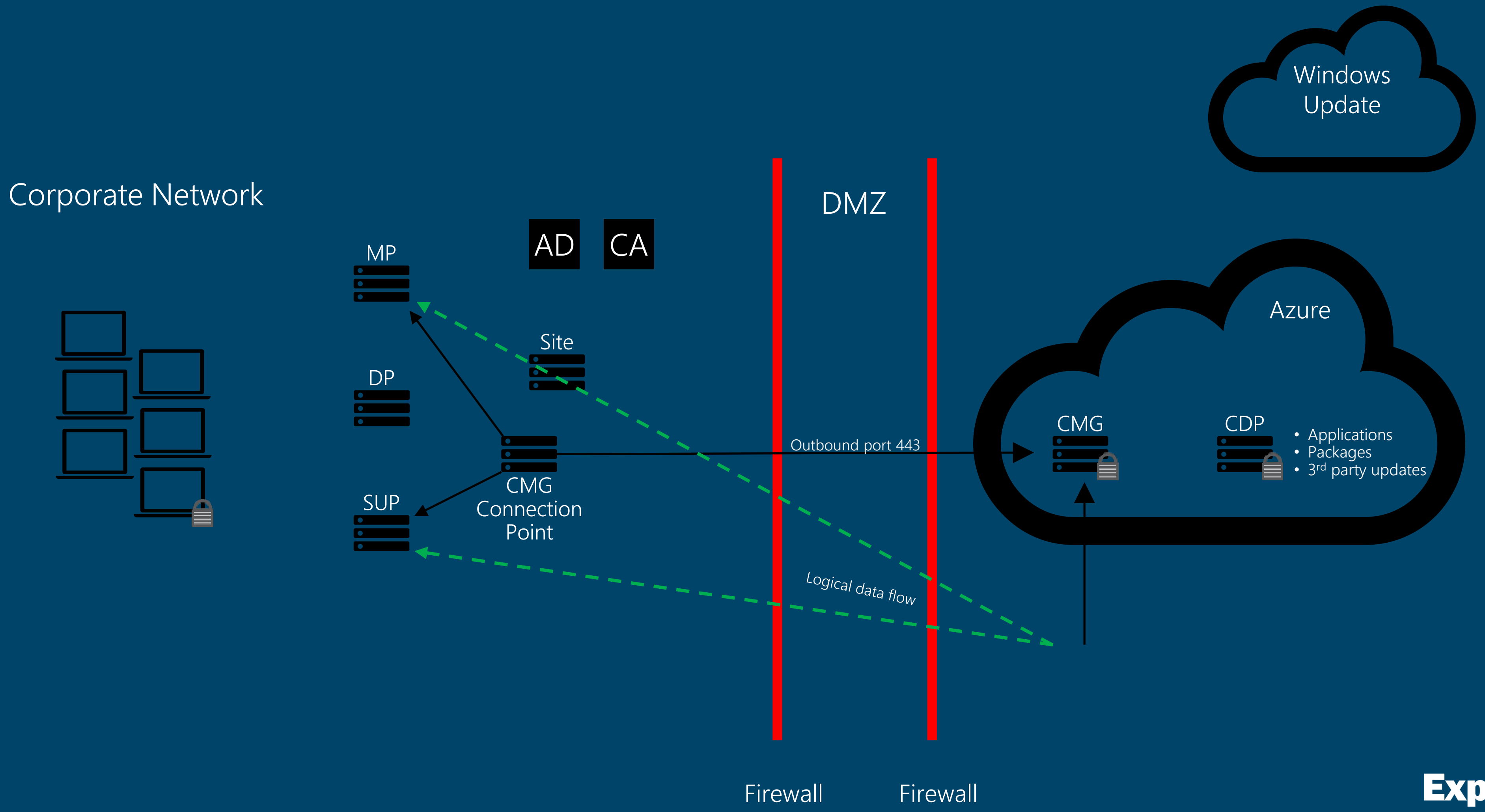
Intune MDM
AD Domain Joined
AAD Joined

ConfigMgr agent
Intune MDM
AD Domain Joined
AAD Joined

Demo

- Configure Hybrid Azure AD Join
- Configure Co-Mgmt
- Windows 10 user experience

Cloud Management Gateway (CMG) – Gateway to heaven…



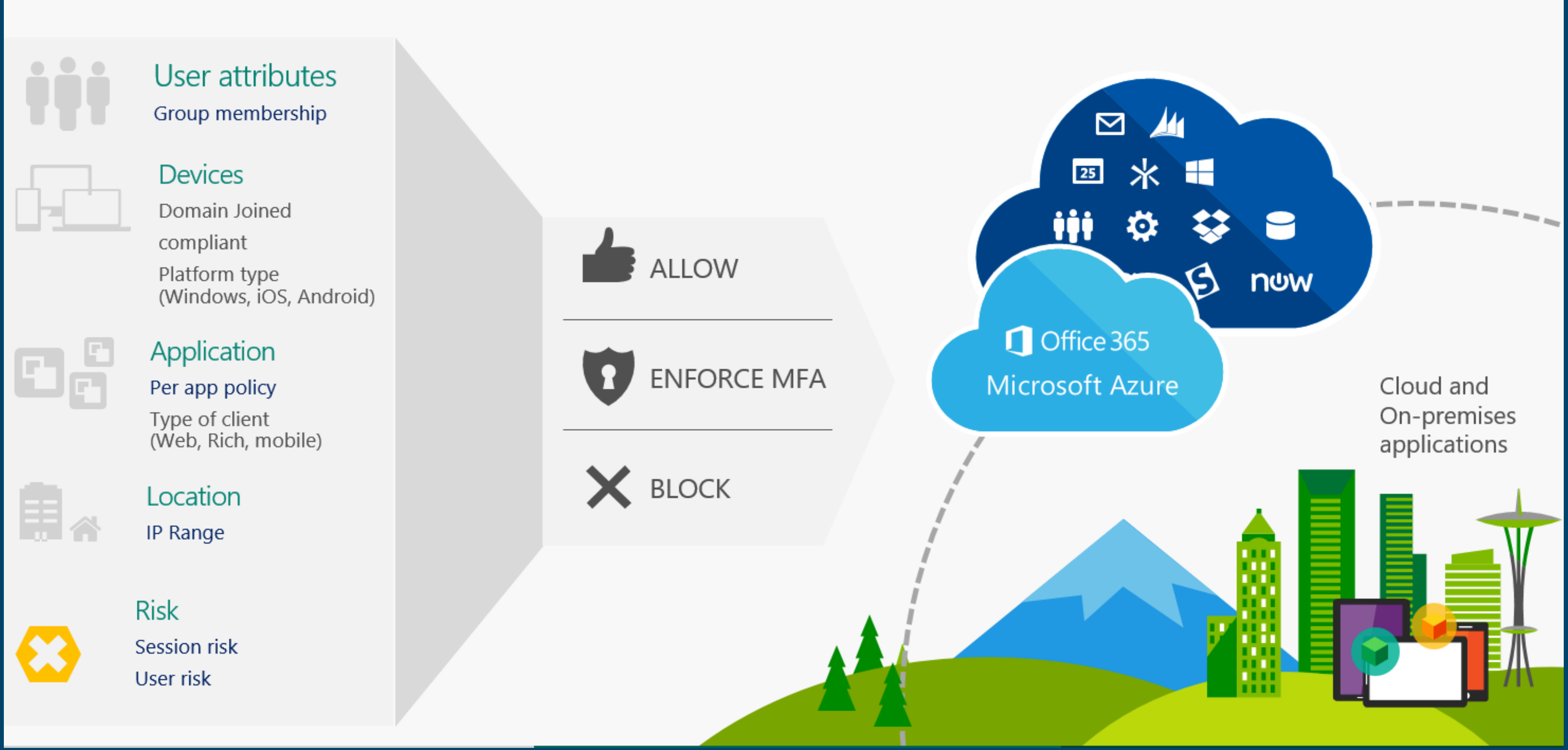
Cloud Management Gateway (CMG) – Gateway to heaven…

- An Azure subscription to host the CMG.
- At least one on-premises Windows server to host the CMG connection point.
- The service connection point must be in online mode.
- A server authentication certificate for the CMG.
- (If using the Azure classic deployment method, you must use an Azure management certificate.)
- Other certificates may be required, depending upon your client OS version and authentication model
  - Aim for Azure AD Token auth and Enhanced HTTP in ConfigMgr
  - Integration with Azure AD may be required for Windows 10 clients.

Demo

- Configure CMG
- Install ConfigMgr Client via Intune

Device based Conditional Access with Intune



User attributes
Group membership

Devices
Domain Joined
compliant
Platform type
(Windows, iOS, Android)

Application
Per app policy
Type of client
(Web, Rich, mobile)

Location
IP Range

Risk
Session risk
User risk

ALLOW

ENFORCE MFA

BLOCK

Cloud and
On-premises
applications

Device based Conditional Access with Intune

Ways to use conditional access with Intune:

- **Device-based conditional access**
- Conditional access for Exchange on-premises
- Conditional access based on network access control
- Conditional access based on device risk
- Conditional access for Windows PCs
  - Corporate-owned
  - Bring your own device (BYOD)
- **App-based conditional access**

Demo

- Device compliance
- Configure Conditional Access
  - Device Based CA on Teams and an Ent. App
  - MFA

Some final (general) notes…

- Always have an «if-shit-hit's-the-fan» strategy when it comes to CA.
  - Microsoft calls it "Break the Glass«

Some final (general) notes…

- Upgrade to Win10 and stay current
- Upgrade to O365 and stay current
- Move to Modern Auth
  - Block Legacy auth
  - https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/enable-or-disable-modern-authentication-in-exchange-online
- Move to Azure AD (Hybrid)
- Upgrade ConfigMgr to the latest and greatest
  - Includes Server OS and SQL if possible

Some final (general) notes…

- On Domain joined devices after Azure AD join, the MDM Autoenrollment (could) take a long time
  - Configure Local or Global MDM Autoenrollment Policy

- Use WMIExplorer to verify settings from Intune MDM (OMA-DM / OMA-URI)
- Use Eventviewer to monitor MDM actions
- Use CCM\Logs to monitor ConfigMgr agent actions
- Use built in reports tool (Advanced Diagnostics Report)

- https://docs.microsoft.com/nb-no/sccm/comanage/overview

Thank You!

Platinum

Microsoft

Gold

audiocodes

Silver

au2mator

pexip

Jabra

logitech