# Move to a modern managed workplace at your own pace!

Arjan Vroege

Peter van der Woude

# Peter van der Woude

Consultant at KPN ICT Consulting

Microsoft MVP for Enterprise Mobility (and Windows Insider)

Happy husband and proud father

COMPAREX
A SoftwareONE Company

KPN ICT Consulting
Sterk in ICT-advies

Microsoft

# Arjan Vroege

Consultant at KPN ICT Consulting

Microsoft MVP for Enterprise Mobility

# Agenda

- Settings the stage
- Architecture and infrastructure
- OS deployment
- Workloads
- Software updates
- Recap

Setting the stage

# Starting point

- **Co-management** – Co-management is about managing Windows 10 devices by using both Configuration Manager and Microsoft Intune
- **Co-existence** – Co-existence is about managing Windows 10 devices by using both Configuration Manager and a third-party MDM
- **Cloud attached** – Cloud attached is about attaching cloud components to the management of Windows 10 devices (think about co-management, Internet clients, Windows-as-a-Service, Windows Analytics)

**COMPAREX**
A SoftwareONE Company

KPN **ICT Consulting**
Sterk in ICT-advies

Microsoft

# Management powered by the M365 Cloud

| | 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 | | ✓ | ✓ |

# Main use cases for co-management

- Flexibility for app deployment and re-evaluation;
- Control over the deployment of quality and feature updates;
- Configuration options via baselines;
- Management capabilities;
- Best of both worlds;

# Movement 1:
## From domain joined to Azure AD joined devices

**AD Domain Joined**

- Extend your on-premises directory with Azure AD.
- Hybrid Azure AD join your AD domain-joined devices
- AD + Azure AD join new devices through Autopilot

**Hybrid Azure AD Joined**

Settings an...
...vices (Enter...
...g of Settings...
...control access...
...e AD device-bas...
...nditional access.
...sers sign-in conver...
...and securely with Windows Hello for Business.

- Transition GPO to MDM
- Pilot Azure AD join to identify AD auth dependencies
- Gradually move traditional management tools that rely on computer identity to their cloud equivalents or AAD enlightened versions (e.g. ConfigMgr with Intune, WSUS to WUfB)
- AAD join new devices (AD joined machines remain AD joined until retired)

**Azure AD Joined**

...te dependency on ...m domain ...ollers

COMPAREX
A SoftwareONE Company

KPN ICT Consulting
Sterk in ICT-advies

Microsoft

MICROSOFT 365

# Movement 2:
## From Configuration Manager to Intune

**Configuration Manger**

- Extend your on-premises infrastructure with CMG.
- Intune enroll existing devices
- Intune enroll and install the ConfigMgr client for new devices through Autopilot

**Co-management**

...the best ...ment capabi... ...orlds ...gets more flexib... ...to the introduct... ...ud ...n can control access... ...Azure AD device-based conditional access.

**Microsoft Intune**

- Transition workloads from Configuration Manager to Microsoft Intune
- Pilot workload transitions to identify management gaps

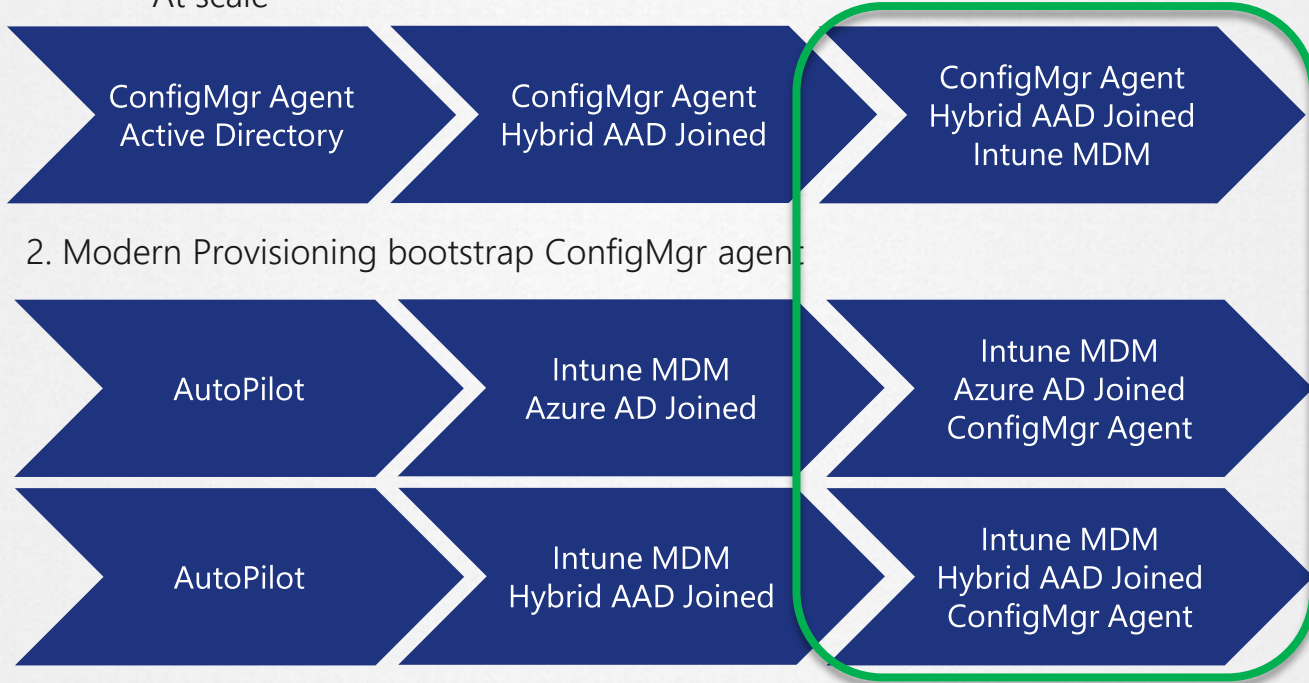...ate dependency on ...em infrastructure ...inate maintenance on ...e infrastructure

COMPAREX
A SoftwareONE Company

KPN ICT Consulting
Sterk in ICT-advies

Microsoft

# Main paths to co-management (existing ConfigMgr)

1. Existing ConfigMgr managed devices auto-enroll into Intune
   - Transparent
   - At scale

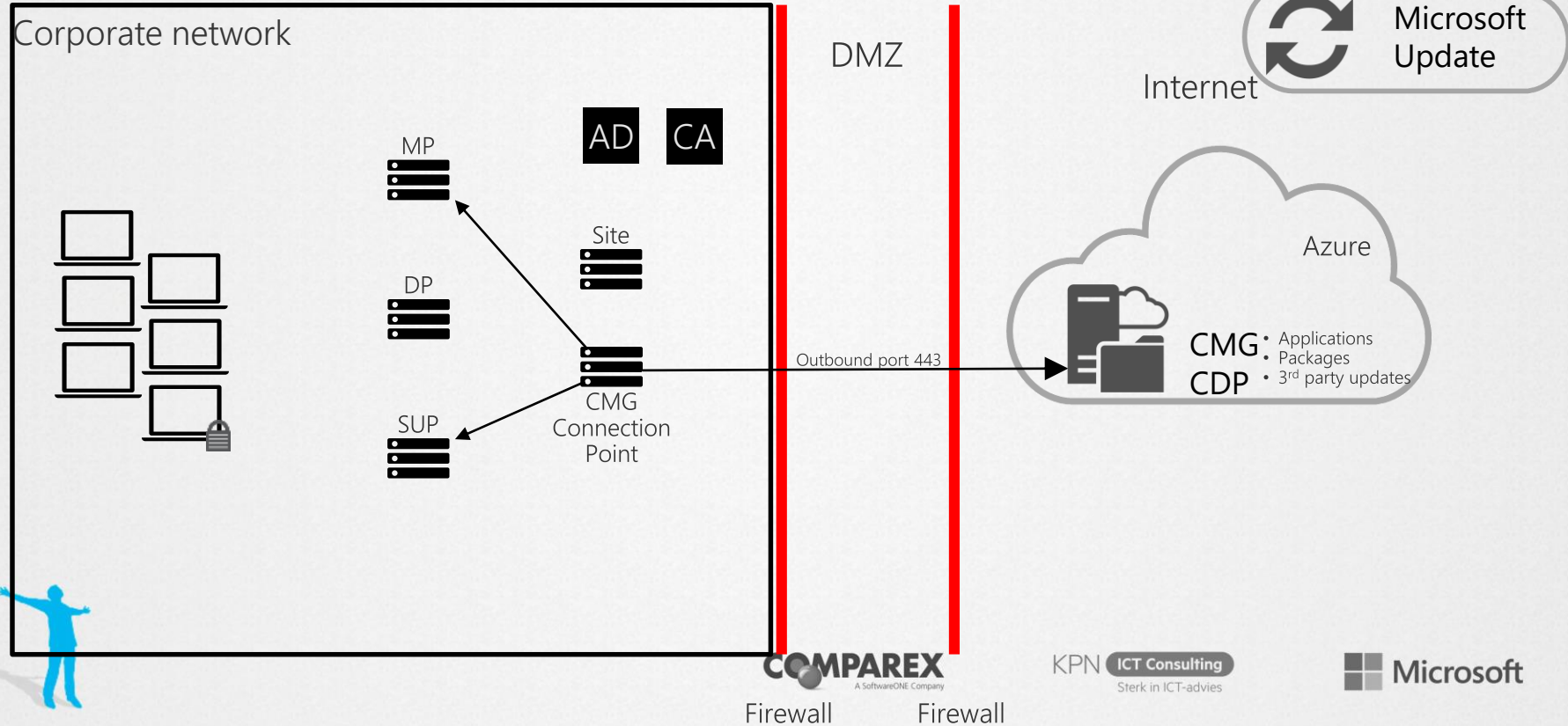| ConfigMgr Agent Active Directory | ConfigMgr Agent Hybrid AAD Joined | ConfigMgr Agent Hybrid AAD Joined Intune MDM |
|---|---|---|

2. Modern Provisioning bootstrap ConfigMgr agent:

| AutoPilot | Intune MDM Azure AD Joined | Intune MDM Azure AD Joined ConfigMgr Agent |
|---|---|---|
| AutoPilot | Intune MDM Hybrid AAD Joined | Intune MDM Hybrid AAD Joined ConfigMgr Agent |

COMPAREX
A SoftwareONE Company

KPN ICT Consulting
Sterk in ICT-advies

Microsoft

Architecture and infrastructure

# Co-Management architecture with ConfigMgr and Intune
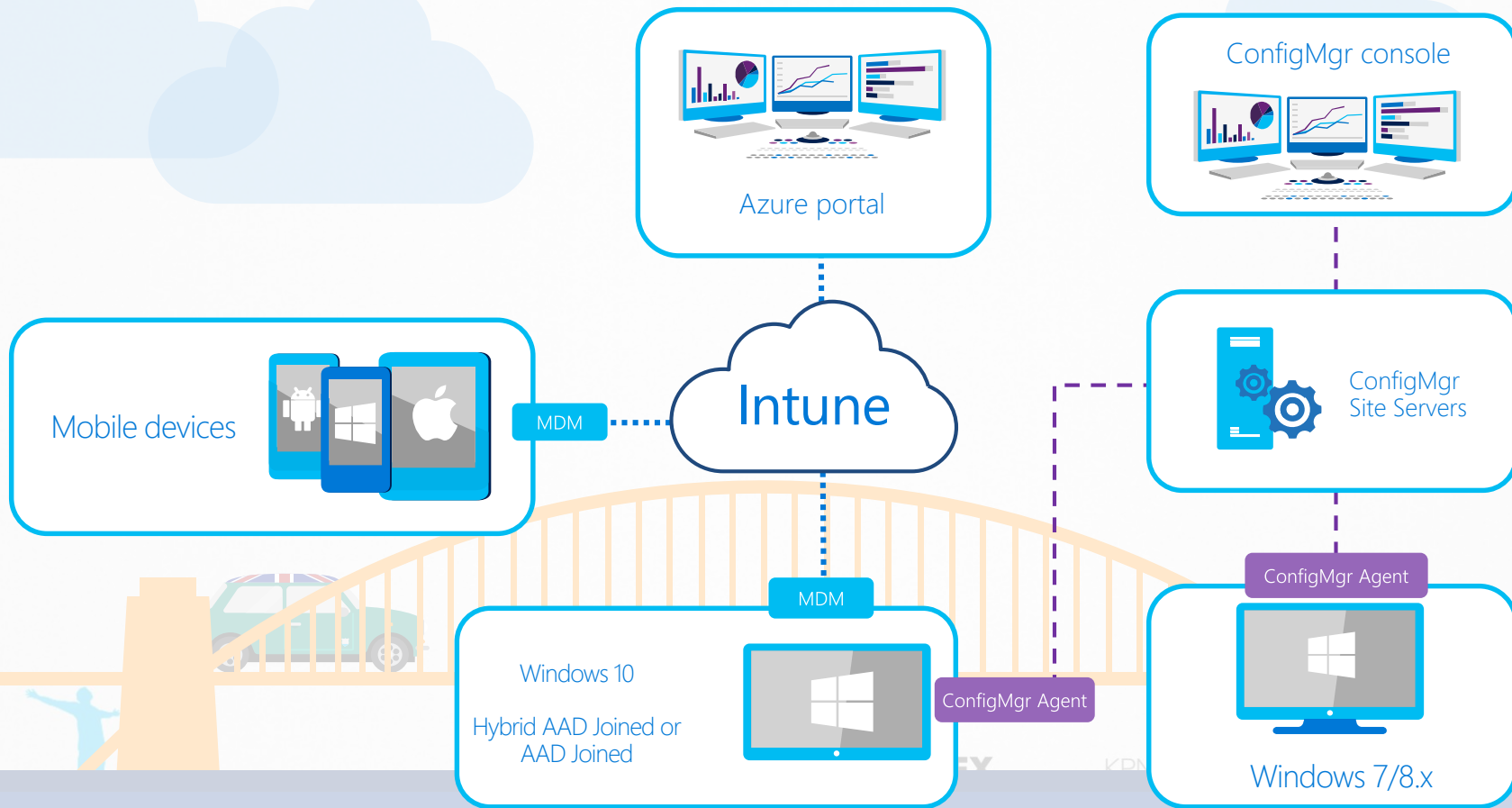
# Cloud management gateway infra

Corporate network

DMZ

Internet

Microsoft Update

AD  CA

MP

Site

DP

Azure

CMG Connection Point

Outbound port 443

SUP

CMG : Applications
· Packages
CDP · 3rd party updates

**COMPAREX**
A SoftwareONE Company

KPN **ICT Consulting**
Sterk in ICT-advies

Microsoft

Firewall     Firewall
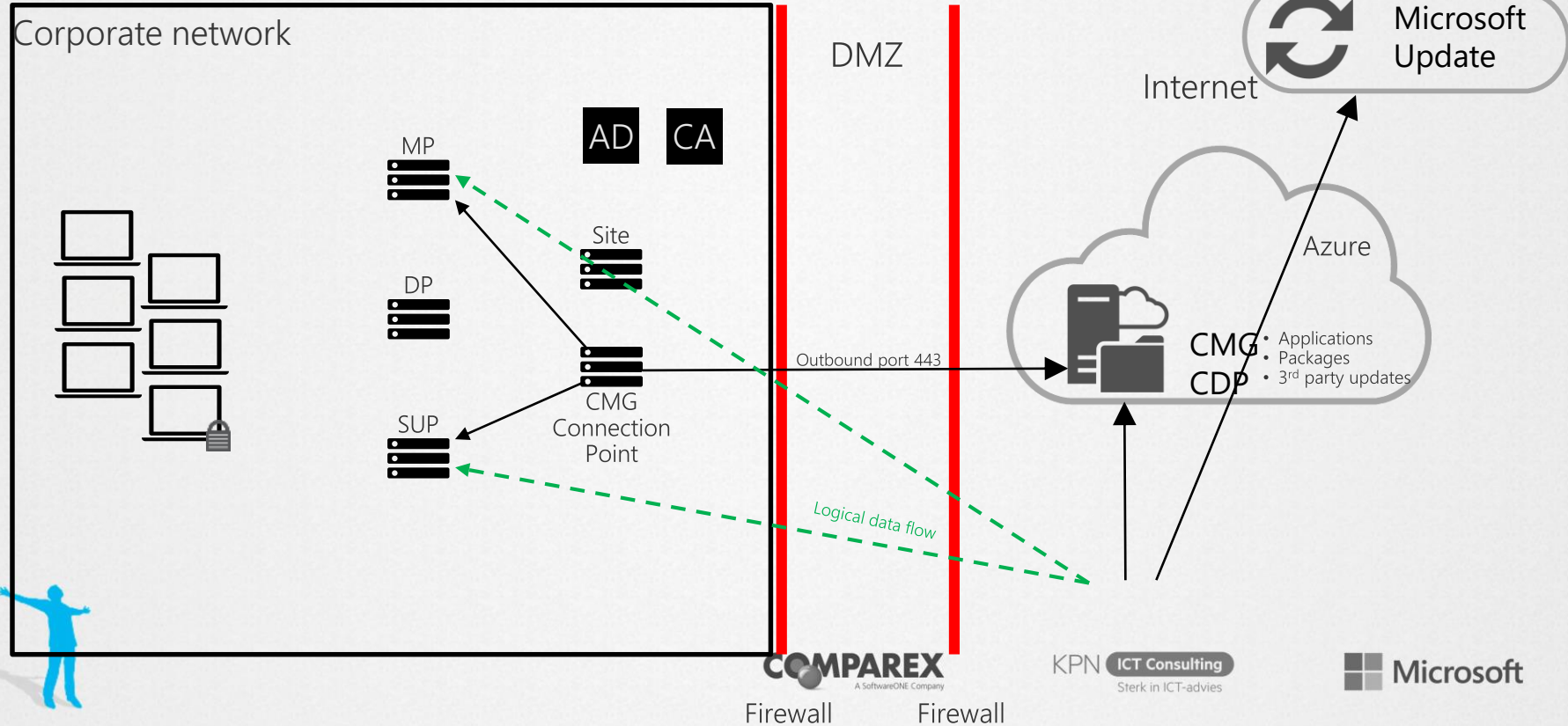
Co-management switching workloads
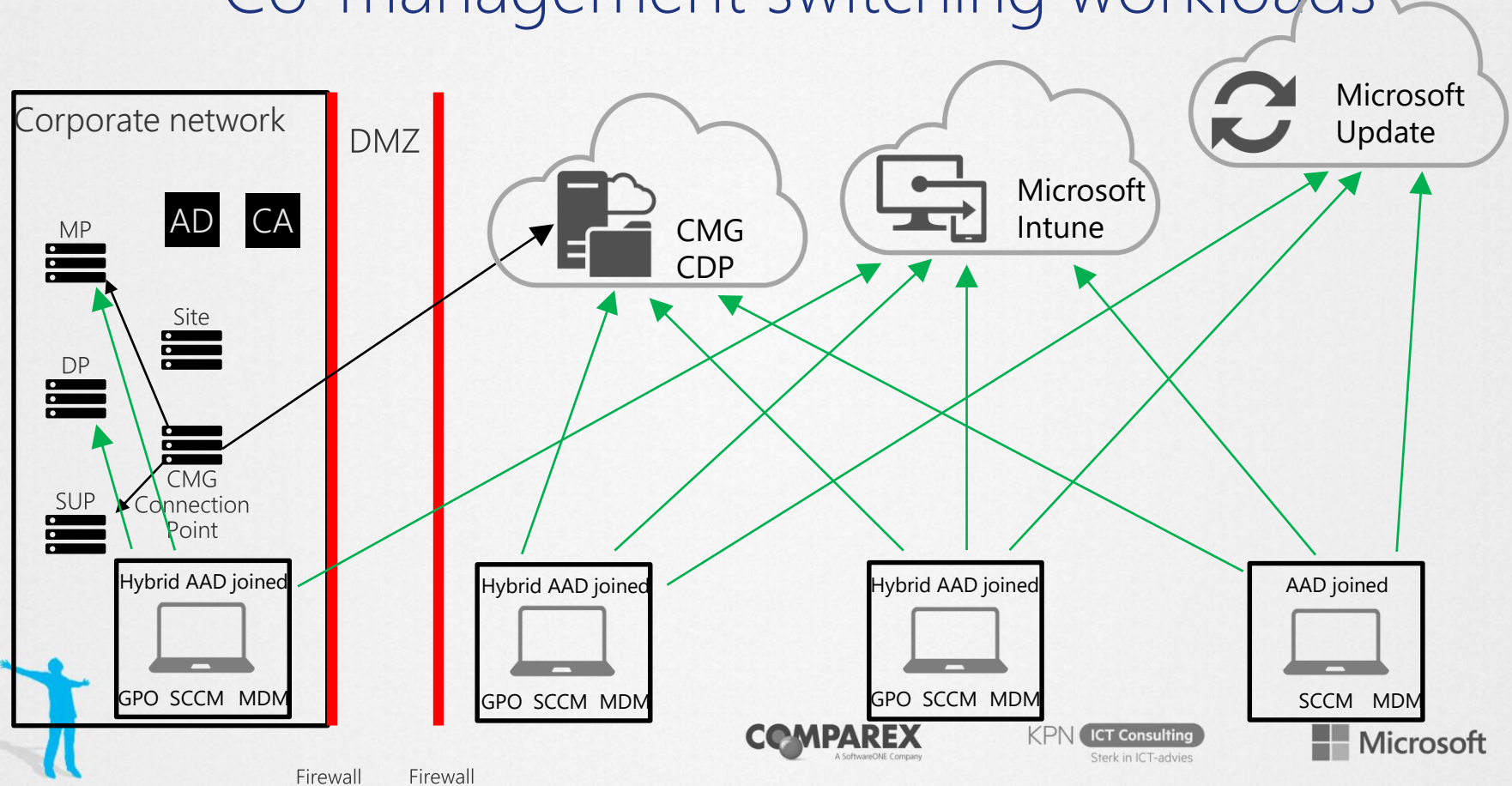
# Management insights

## Insights on Cloud Attach Readiness

- Provide guided assessment on the readiness to attach to the cloud
- Direct action based on the assessment

# Demo: Management Insights

# OS Deployment
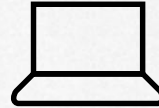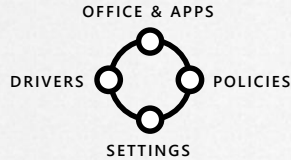
# Windows deployment

## Traditional

OFFICE & APPS

DRIVERS              POLICIES

SETTINGS

Build a custom image, gathering everything else that's necessary to deploy

**+**

Deploy image to a new computer, overwriting what was originally on it

**=**

Time means money, making this an expensive proposition

## Modern

Un-box and turn on off-the-shelf Windows PC

**+**

Transform with minimal user interaction

**=**

Device is ready for productive use

COMPAREX
A SoftwareONE Company

KPN ICT Consulting
Sterk in ICT-advies

Microsoft

# Windows deployment

**Traditional**

OFFICE & APPS
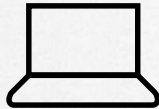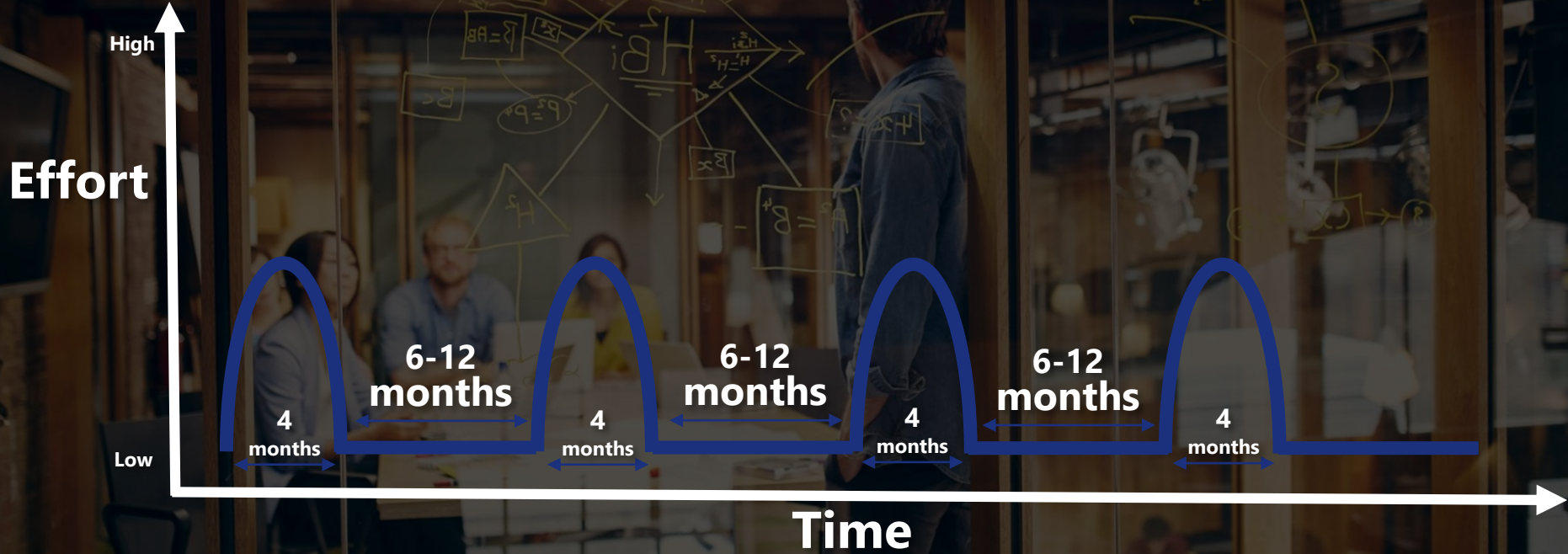
DRIVERS      POLICIES

SETTINGS

Build a custom image, gathering everything else that's necessary to deploy

**+**

Deploy image to a new computer, overwriting what was originally on it

**=**

Time means money, making this an expensive proposition

**Hybrid**          OR

**Modern**
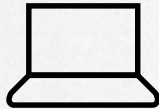
Un-box and turn on off-the-shelf Windows PC

**+**

Transform with minimal user interaction
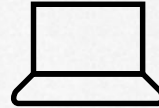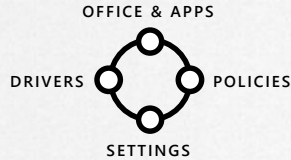
**=**

Device is ready for productive use

COMPAREX
A SoftwareONE Company

KPN ICT Consulting
Sterk in ICT-advies

Microsoft

# Hybrid AzureAD Join
## What and Why?

**What:**

- Devices joined to your local Active Directory and registered in AzureAD;

- With AAD Connect and Windows 10 1607 or later you're already using it

- Referred as DJ++

**Why:**

- To benefit from the capabilities provided by Azure Active Directory;

- To migrate your workloads one-by-one;

# Hybrid AzureAD Join
## How?



AD Domain Controller

Offline Domain Join Connector

Intune

Windows Autopilot Deployment Service

Complete join over corp net

Receive GPOs over corp net

Receive ODJ

MDM enrollment

Autopilot profile

Hardware ID

Employee unboxes device, self-deploys
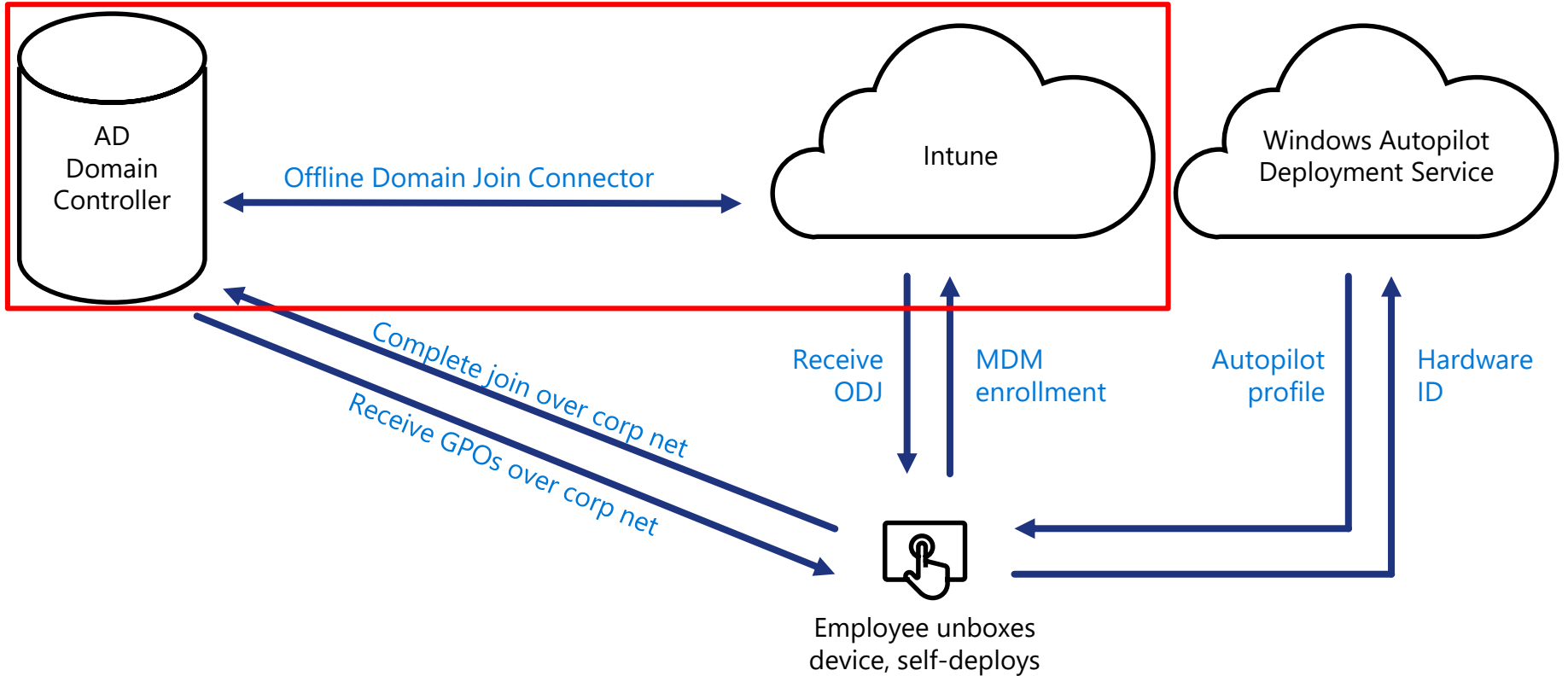
# Hybrid AzureAD Join
And what now?

- Create a Autopilot Profile and choose Hybrid Azure AD Join;

- Deploy the ConfigMgr client to the enrolled computer;

- Deploy:
  - Tasks sequence through CMG from ConfigMgr;
  - Applications and Settings from Intune;

# Windows Autopilot Scenario's

User-Driven:
- Hybrid Joined or AzureAD only supported;
- Designed to transform the initial state to a ready device for the user;
- User needs to provide his credentials;

Self-Deploying:
- Hybrid Joined not supported only AzurAD Joined;
- Designed for Kiosk, digital signage device, or a shared device;
- No credentials needed, automatically joined to AAD;

COMPAREX
A SoftwareONE Company

KPN ICT Consulting
Sterk in ICT-advies

Microsoft

# OS Deployment through CMG

**Possibilities:**

- Windows 10 in in-place upgrades
- Task sequences which are not using boot images

**Requirements:**

- Configuration Manager 1802 or later;
- TS deployed with option '**Download all content locally before starting task sequence**'

COMPAREX
A SoftwareONE Company

KPN ICT Consulting
Sterk in ICT-advies

Microsoft

# Demo:
# OS Deployment
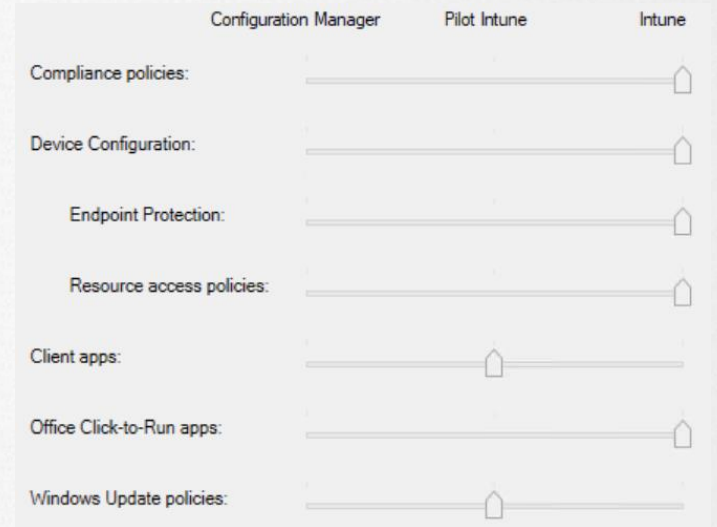
# Workloads

# Overview of workloads

- Compliance policies
- Device configuration
- Client apps
- Office Click-to-Run apps
- Windows update policies



| | Configuration Manager | Pilot Intune | Intune |
|---|---|---|---|
| Compliance policies: | | | ⌂ |
| Device Configuration: | | | ⌂ |
| Endpoint Protection: | | | ⌂ |
| Resource access policies: | | | ⌂ |
| Client apps: | | ⌂ | |
| Office Click-to-Run apps: | | | ⌂ |
| Windows Update policies: | | ⌂ | |

# Compliance Policy

- Authority for checking Device Compliance
- Device Compliance state can be used in Conditional Access policies;
- Device Compliance state can be used to report or monitor the device states;
- Both ConfigMgr and Intune will update the compliance state of the device in AzureAD

# Compliance Policy
## *Compare ConfigMgr and Intune*

ConfigMgr:
- Device Health Attestation
  - Bitlocker, Secure Boot, Code Integrity, Early Launch Antimalware
- Require Windows Update for Business compliance;
- Require registration within AzureAD;
- Require All required updates;
- Require All required applications;

Intune:
- Device Health Attestation
  - Bitlocker, Secure Boot, Code Integrity
- Device Properties like OS versions and OS build ranges;
- Require device compliance from ConfigMgr;
- System Security like Password, Encryption, Firewall, Antivirus and Antispyware;
- Windows Defender (ATP)

COMPAREX
A SoftwareONE Company

KPN ICT Consulting
Sterk in ICT-advies

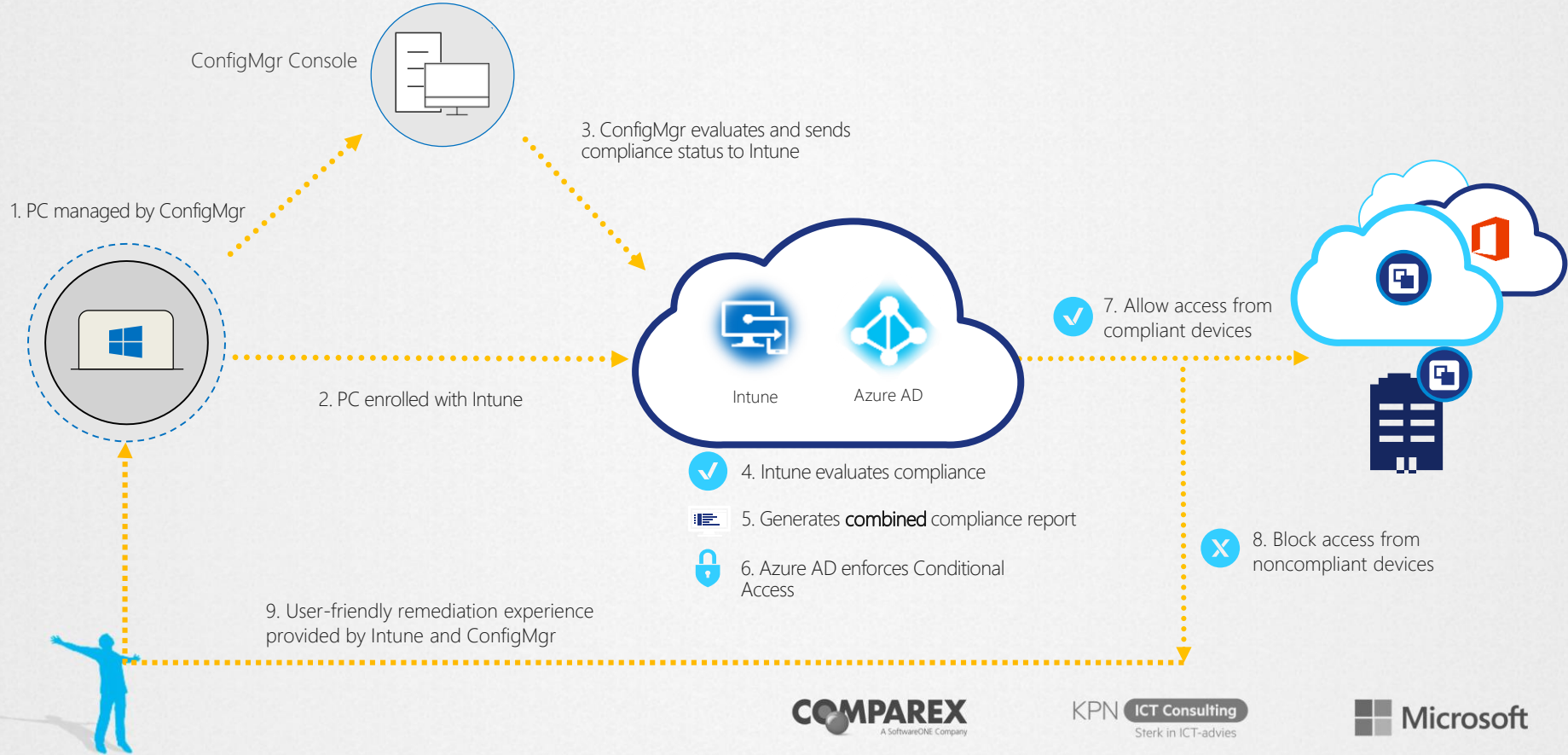Microsoft

# Compliance Policy
*Moving from ConfigMgr to Intune*

- Create (migrate) your Device Compliance policies to Microsoft Intune;

- Define Pilot machines to test the new Compliance Policies;

- Run a pilot on those devices;

- Flip-the-switch for Device Compliance in ConfigMgr

COMPAREX
A SoftwareONE Company

KPN ICT Consulting
Sterk in ICT-advies

Microsoft

# Hybrid Device Compliance
## ConfigMgr compliance policies as part of Intune assessment

MICROSOFT 365

ConfigMgr Console

3. ConfigMgr evaluates and sends compliance status to Intune

1. PC managed by ConfigMgr

2. PC enrolled with Intune

Intune

Azure AD

7. Allow access from compliant devices

4. Intune evaluates compliance

5. Generates **combined** compliance report

6. Azure AD enforces Conditional Access

8. Block access from noncompliant devices

9. User-friendly remediation experience provided by Intune and ConfigMgr

COMPAREX
A SoftwareONE Company

KPN ICT Consulting
Sterk in ICT-advies

Microsoft

# Device Configuration
*Moving from ConfigMgr to Intune*

- Create your Resource Acces policies in Microsoft Intune;
- Define Pilot machines to test the new Device Configuration policies;
- Run a pilot on those devices;
- Flip-the-switch for Device Configuration in ConfigMgr

# Device Configuration
## *What about my Group Policies?*

- Group policies can still be used in a co-managed scenario;

- Re-think your Group Policy (setting) strategy;

- Do not focus on a 1-on-1 to MDM strategy;

- Evaluating existing Group Policies with MDM Migration Analysis Tool (MMAT)

**COMPAREX**
A SoftwareONE Company

**KPN** ICT Consulting
Sterk in ICT-advies

Microsoft

# Office Click-to-Run apps

- What
    - Starting in Configuration Manager 1806, this workload manages Office 365 apps on co-managed devices
    - After moving the workload, the app shows up in the Company Portal on the device
    - Office updates may take around 24 hours to show up on client unless the devices are restarted
    - There's a new global condition, Are Office 365 applications managed by Intune on the device. This condition is added by default as a requirement to new Office 365 applications. When you transition this workload, co-managed clients don't meet the requirement on the application. Then they don't install Office 365 deployed via Configuration Manager.

# Office Click-to-Run apps

- Why
  - Office CTR deployment requirements
  - Control for targeting Office CTR deployments
  - Manageability for Office CTR

# Office Click-to-Run apps

- Switch
  - Create the Office CTR apps in Microsoft Intune;
  - Define Pilot machines to test the new Office CTR deployment;
  - Run a pilot on those devices;
  - Verify the existence and usage of the new global condition;
  - Flip-the-switch for Office Click-to-Run apps in ConfigMgr

COMPAREX
A SoftwareONE Company

KPN ICT Consulting
Sterk in ICT-advies

Microsoft

# Client apps

- What
    - Starting in Configuration Manager version 1806, it's possible to use Intune to manage client apps on co-managed Windows 10 devices.
    - Transition this workload, will make that any available apps that are deployed from Intune available in the Company Portal. Apps that are deployed from Configuration Manager are available in Software Center.
    - Pre-release feature

**COMPAREX**
A SoftwareONE Company

KPN **ICT Consulting**
Sterk in ICT-advies

Microsoft

# Client apps

- Why
  - Application deployment requirements (think about re-evaluation, supersedence)
  - Control for targeting deployments
  - Troubleshooting
  - (Closing the gap)

# Client apps

- Switch
  - Create the client apps in Microsoft Intune;
  - Define Pilot machines to test the new client app deployment;
  - Run a pilot on those devices;
  - Verify if the client app deployment needs can be met by using Intune
  - Flip-the-switch for Office Click-to-Run apps in ConfigMgr

COMPAREX
A SoftwareONE Company

KPN ICT Consulting
Sterk in ICT-advies

Microsoft

# Windows Update Policies

- What
  - Switching to Windows Update for Business
  - Monitoring from ConfigMgr to Intune of Windows Analytics
  - Define Update Policies for your devices;
  - Moving from on-premise fine grained control to only defining channels (less control);

COMPAREX
A SoftwareONE Company

KPN ICT Consulting
Sterk in ICT-advies

Microsoft

# Windows Update Policies

- Why
  - Reduce time of controlling deployment of update;
  - Rely on Windows Update cloud functionality for delivering updates;
  - Be ready for Windows-as-Service

# Windows Update Policies

- Switch
  - Define your Windows Update for Business policies within Intune
  - Define Pilot machines to test the new policies;
  - Run a pilot on those devices;
  - Verify if the policy is applied and active;
  - Flip-the-switch for Windows Update Policies in ConfigMgr

# Wrap up

# Cool tip: CMPivot

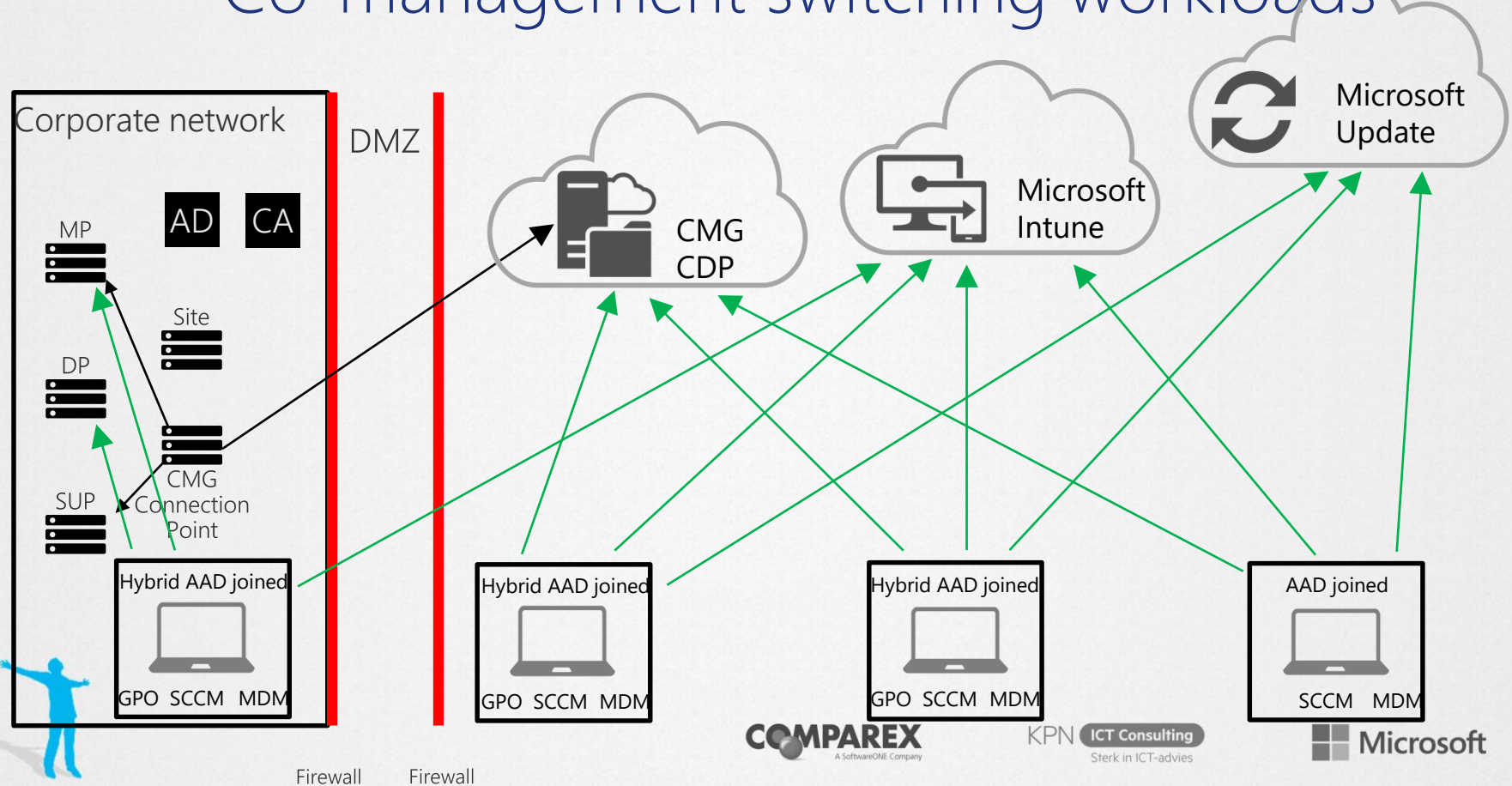- Co-managed devices can be queried by using CMPivot. Even when those devices are only available on the Internet.

COMPAREX
A SoftwareONE Company

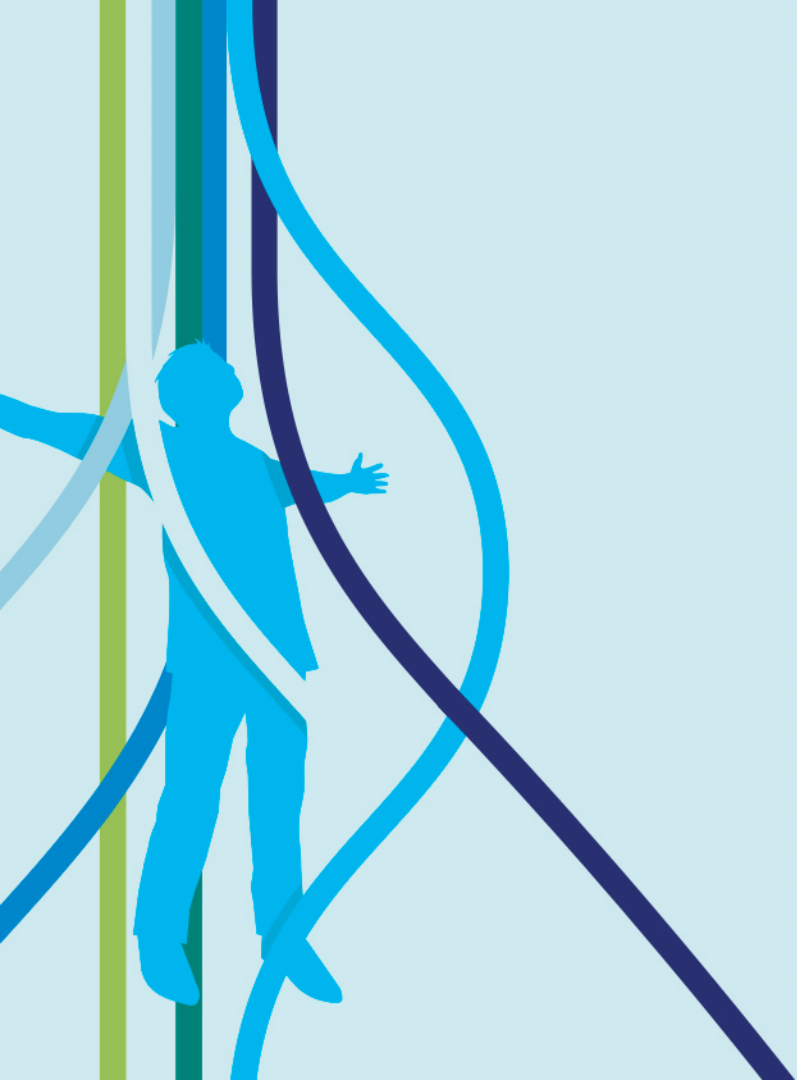KPN ICT Consulting
Sterk in ICT-advies

Microsoft

# So why are you here?

You have invested a lot in ConfigMgr. It works great.
Now you want incremental cloud-value.

## Good news!

ConfigMgr will be available as long as you need it.

ConfigMgr has easy access to M365 cloud-value.

**COMPAREX**
A SoftwareONE Company

KPN **ICT Consulting**
Sterk in ICT-advies

Microsoft

# Move to a modern managed workplace at your own pace!

Many organizations want to make the switch to a modern managed workplace, but are currently unable to make the complete switch. Often this is related to missing specific management features, like limited control over updates and missing rich app deployment features. The good news is that it's not required to directly make the complete switch. This can be achieved in steps, by using Configuration Manager and Microsoft Intune. In this session we will present and show you how to use these tools in combination with Windows 10 to make a smooth transition.

COMPAREX
A SoftwareONE Company

KPN ICT Consulting
Sterk in ICT-advies

Microsoft

# Move to a modern managed workplace at your own pace!

Introduction to moving to a modern managed workplace (Peter)
- Setting the scope of the session by
- defining a modern managed workplace
- defining the different use cases for managing devices via either ConfigMgr, Microsoft Intune, or both

Co-management (Peter)
- Minimal requirements, enablement and workloads
- Infrastructure requirements, CMG
- **Cost calculator including DEMO**
- Pushing the ConfigMgr client via Microsoft Intune
- Show the client behavior in the logs

OS deployment (Arjan)
- Movement towards Windows Autopilot
- Differentiating between Azure AD join and hybrid Azure AD join
- In-place upgrade scenario

Compliance policies > Device compliance (Arjan)
- Switch compliance policies from ConfigMgr to Microsoft Intune
- After switching, Microsoft Intune can still get data via the ConfigMgr client and MDM (separate compliance check in Intune)
  - Useful when checking for specific updates and specific apps
- Show the client behavior in the logs

Configuration baselines > Device configuration (Arjan)
- Switch configuration baselines from ConfigMgr to Microsoft
- After switching, ConfigMgr can still enforce specific settings (separate baseline check in ConfigMgr)
- Useful for enforcing specific settings
- Show the client behavior in the logs

Apps (Peter)
- Switch Office Click-to-Run apps from ConfigMgr to Microsoft Intune (check the global condition)
- Switch Client apps from ConfigMgr to Microsoft Intune to get apps available in Software Center and Company Portal (preview)

Software updates (Arjan/Peter)
- Switch updates from ConfigMgr to Windows Update for Business
- Verify the impact of dual scan
- Reporting can be a good use case for Windows Analytics
- Show the client behavior in the logs

Summarization of moving to a modern managed workplace (Peter)
- Concluding the scope of the session by plotting the different management capabilities on the different use cases

COMPAREX
A SoftwareONE Company

KPN ICT Consulting
Sterk in ICT-advies

Microsoft

Explain workload

Explain usage of workload

Explain move workload to cloud

# Windows Update policies

- What

- Why

- Switch

COMPAREX
A SoftwareONE Company

KPN **ICT Consulting**
Sterk in ICT-advies

Microsoft