coretech

# Microsoft
# Enterprise Mobility Suite

# Kent Agerlund

coretech


@Agerlund

Chief Technical Architect @ Coretech Global

Blog.coretech.dk /author/kea

Microsoft® Most Valuable Professional

Enterprise Mobility MVP

# Marius A. Skovli

coretech

@MariusSkovli

Managing Consultant

11+ years of experience with Microsoft Enterprise Client Management

scug.no
cmsource.net
blog.coretech.dk


Microsoft Solution Expert

coretech

# Data Ecosystem

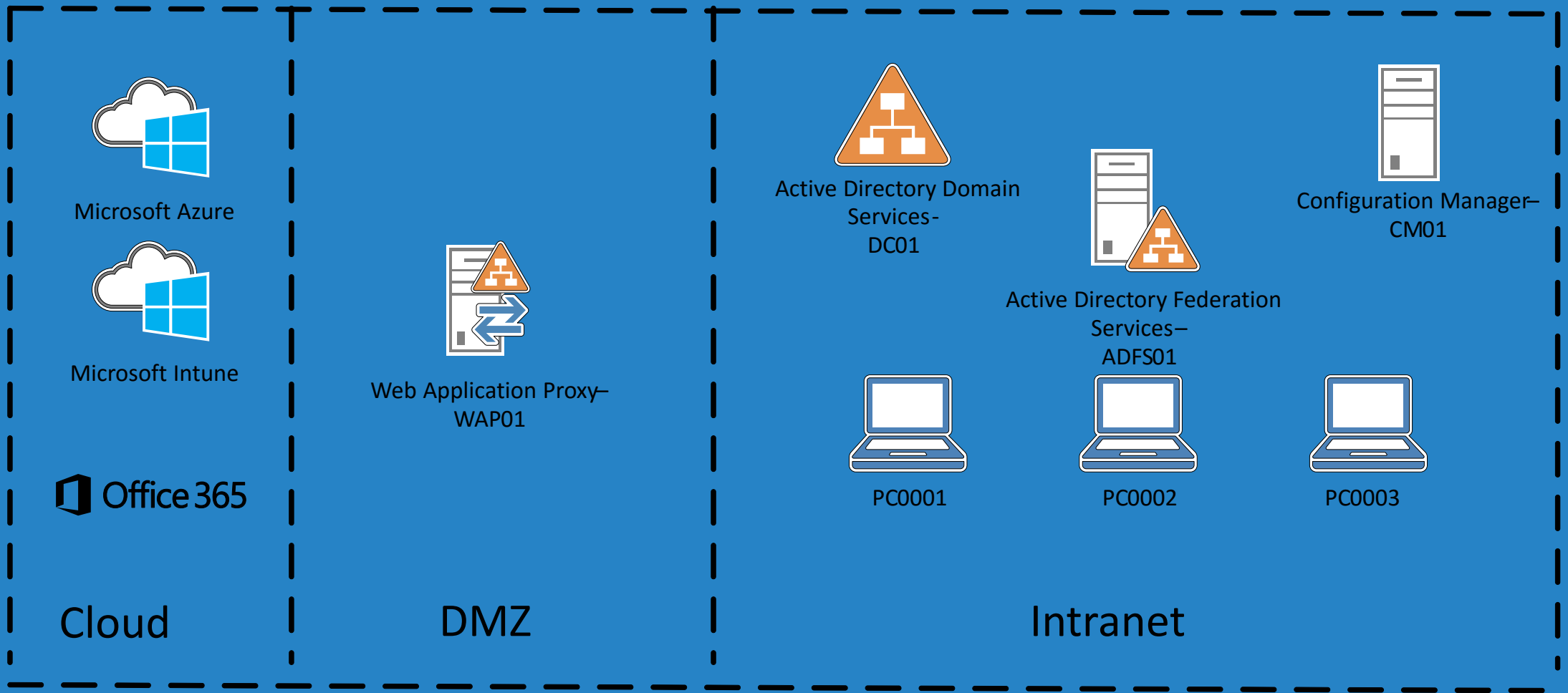
WHO

HOW

WHERE

AGE

# The demo environment



coretech

# Building your EMS LAB

- Outlook account - http://bit.ly/CTOutlook
- Azure Pass - http://bit.ly/CTAzurePass
- OR
- Azure Trial - http://bit.ly/CTAzureTrial
- Register your public domain
- Sign up to Office 365 using YOURDOMAIN.ONMICROSOFT.COM - http://bit.ly/CTO365
- Sign up for EMS http://ref.ms/ems
- Sign up to Intune Trial using YOURDOMAIN.ONMICROSOFT.COM - http://bit.ly/CTIntune

- Accounts:
  - Service account for Azure Active Directory synchronization
  - Global Azure Active Directory Administrator
  - Office 365 Administrator
  - Microsoft Intune Administrator
  - Apple ID's
  - Microsoft Account
  - Google ID

coretech

# 10 Steps for a Successful Mobile Deployment

coretech

# 1 – Secure a Sponsor

1. Why a good sponsor is important?
   - Resources
   - Escalations
   - New standards and policies
2. How to find the best sponsor?
   - Who will profit most
   - Show business value
   - Come well prepared

coretech

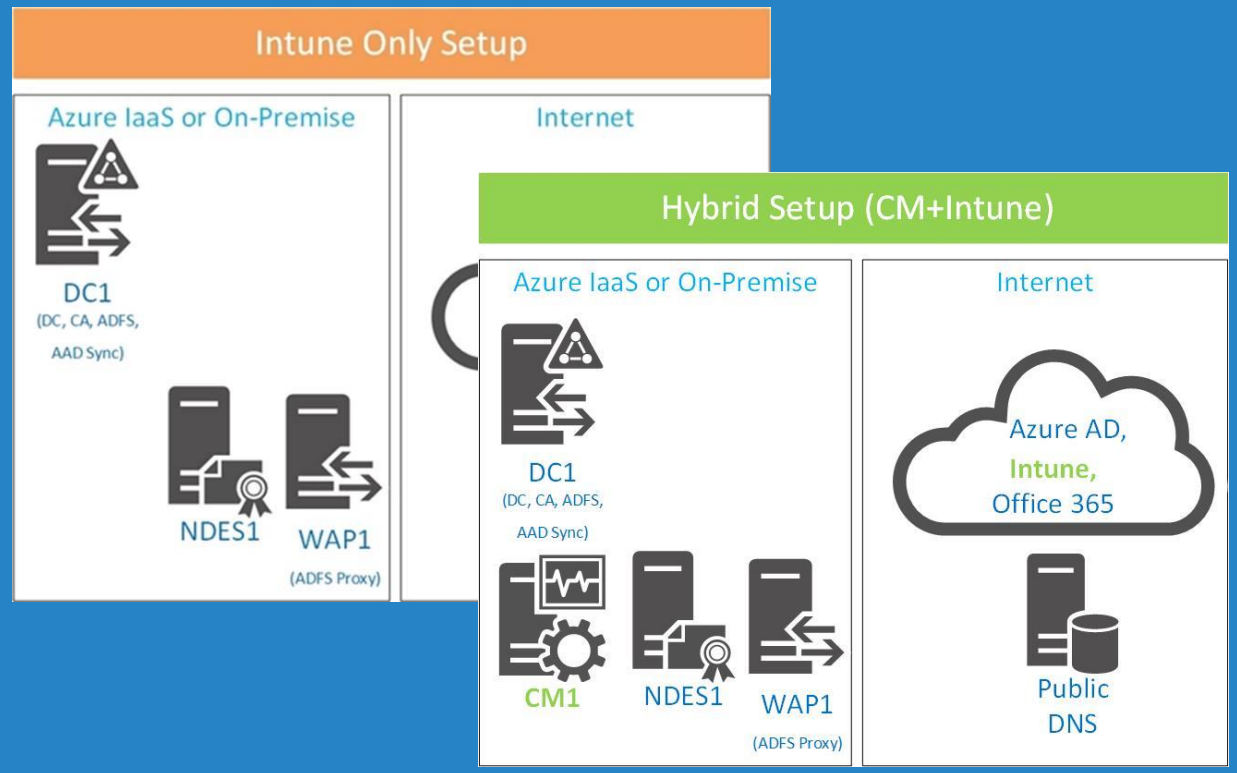
# 2 - Define your starting point and end-goal

- Ask **the Business** for their functional data protection needs
  - Common Understanding
  - Define the End-Goal (Not Technical!)
  - Pre-defined Questionnaire and Requirements list
  - Quantify requirements based on business impact
  - Structure Requirements
    - Personas
    - Scenario's and Processes
    - Business Impact and Success
    - Applications and Data required to become mobile
- Ask IT for their (non-functional) data protection needs
  - Common Understanding
  - Agree on the End-Goal
  - Pre-defined Questionnaire and Requirements list
  - Quantify requirements based on business impact
  - Structure Your Requirements
    - Identity
    - MDM
    - MAM
    - Security, etc.

coretech

# 3 – Setup a Test Environment

1. Proof – Validate Requirements
2. Identify issues and gaps early
3. Education
4. Build Your Own Enterprise Mobility Lab



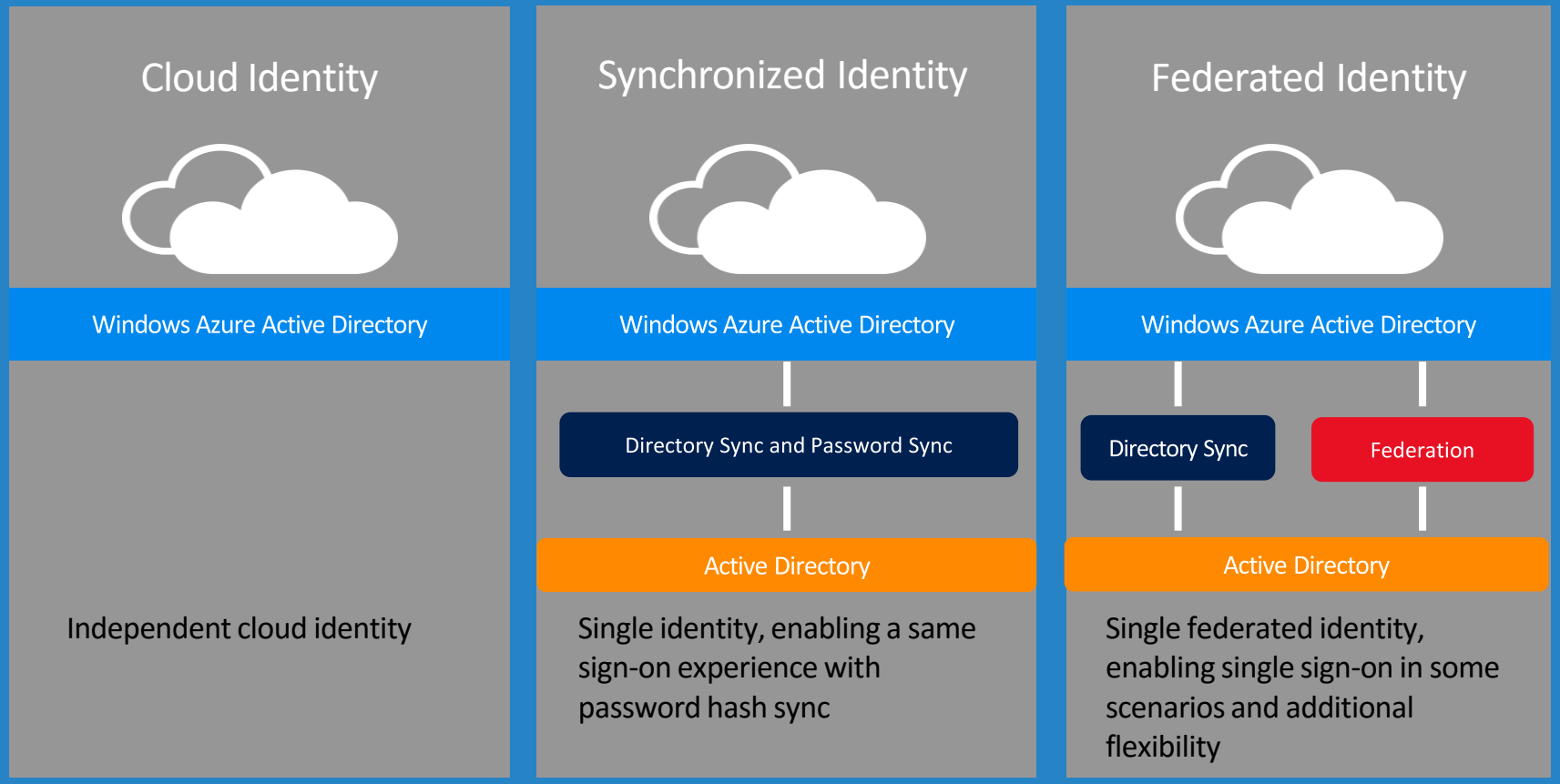
coretech

# 4 Assemble the correct team

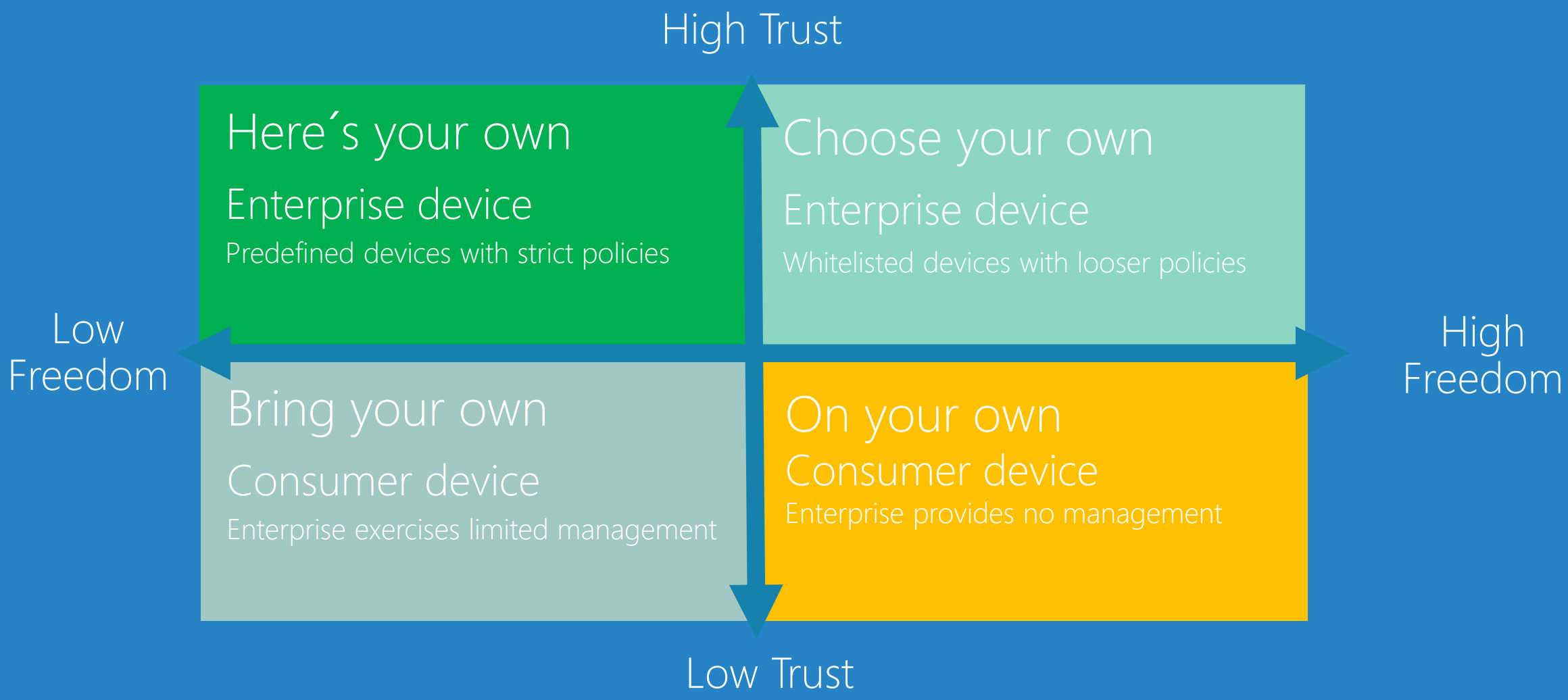
- PKI
- Identity
- Network
- Productivity
- Data protection

coretech

# 5 - The right Identity Solution



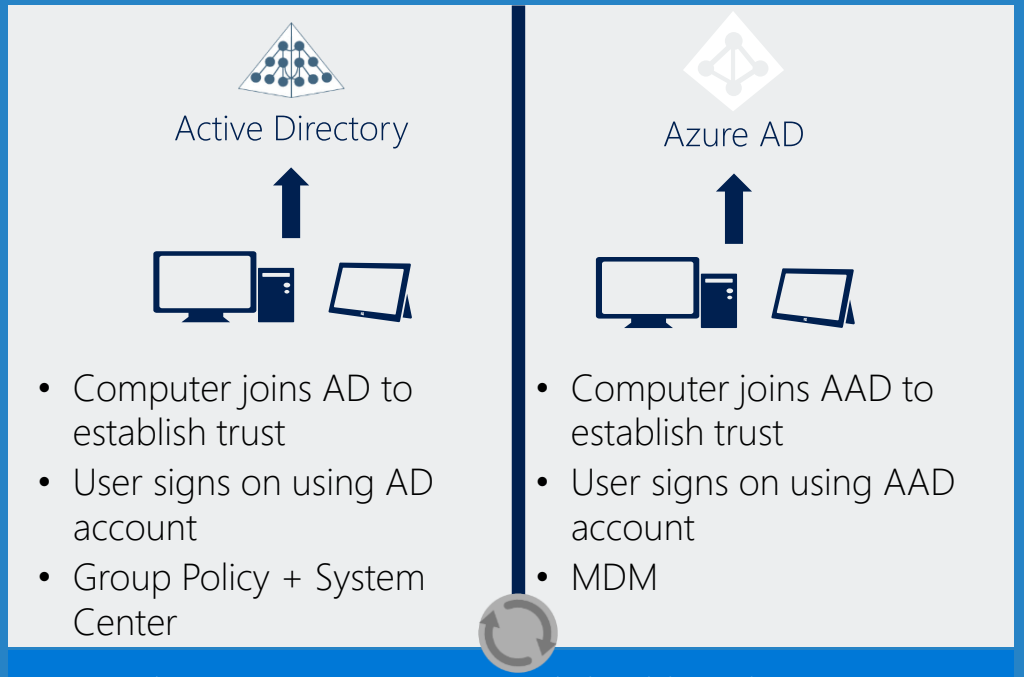
# 6 – Mobile Device Management




*Source: Enterprise Mobility Suite Managing BYOD and Company-Owned Devices*

# 7 - Enrollment Options

## ORGANIZATION OWNED

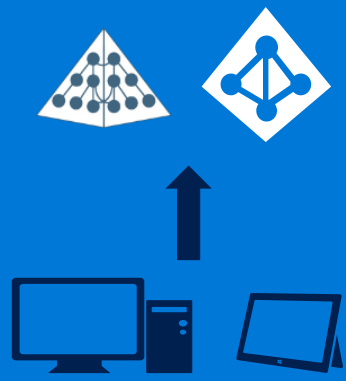



- Computer joins AD to establish trust
- User signs on using AD account
- Group Policy + System Center

- Computer joins AAD to establish trust
- User signs on using AAD account
- MDM

- Single sign-on to enterprise and cloud-based services

## PERSONALLY OWNED (BYOD)



- Computer registers with AAD via Workplace Join to establish trust for remote resource access
- User signs in with a Microsoft account, associates an AAD account
- MDM

coretech

# 8 - Data Protection

- How to prevent access to Company data by non-compliant mobile devices
  - Insecure devices put your company data at risk
- Keep Company data separate from Personal Data
  - Company owned data should be protected and controlled
- End users don't like "Containerized" solutions
  - Users prefer to work with applications they are familiar with (e.g. Mail, Web browser, File Explorer)
  - Users don't like to switch between different environments on the same device
- How to prevent data loss by lost devices and unenrolled (BYOD) devices
  - Ensure Company Data will be wiped or is unaccusable

coretech

# 9 - Work from Anywhere from any Device

- Authentication
- Trust
- Device types
- *Define anywhere*

coretech

# 10 - Make your Applications mobile and manageable

- Stores
- Personal vs Company
- Data protection

coretech

# At the end of the day



## USERS

Users expect to be able to work in any location and have access to all their work resources.

## DEVICES

The explosion of devices has eradicated the standards-based approach to corporate IT.

## APPS

Deploying and managing apps across personal and organization-owned devices is difficult.

## DATA

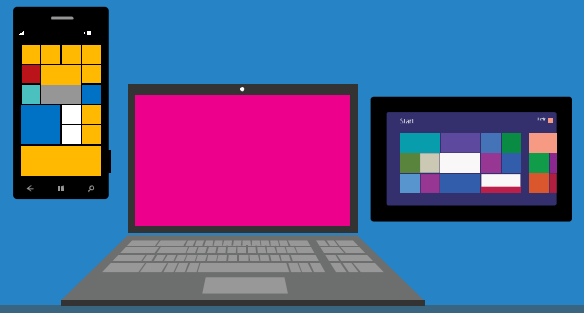
Enabling users to be productive while maintaining compliance and reducing risk.

coretech

# Enterprise Mobility Suite (EMS)

## Not a single product, but several Cloud services

| Azure Active Directory Premium | Microsoft Intune | Azure Rights Management Service | Microsoft Advanced Threat Analytics |
|---|---|---|---|



coretech

# What's included in Azure AD

| Feature | Free | Basic | Premium |
|---|---|---|---|
| Directory as a Service | ✓ | ✓ | ✓ |
| Azure AD Connect | ✓ | ✓ | ✓ |
| 99.9% Uptime SLA | × | ✓ | ✓ |
| Branding | × | ✓ | ✓ |
| Self Service Password Reset | × | ✓ | ✓ |
| Application Proxy | × | ✓ | ✓ |
| Microsoft Identity Manager | × | × | ✓ |
| Self Service Password Reset (write back to On Premises) | × | × | ✓ |
| Advanced Security Reports | × | × | ✓ |
| Multi Factor Authentication | × | × | ✓ |

https://azure.microsoft.com/en-us/documentation/articles/active-directory-editions/.

coretech

# Demo

## Azure Active Directory

coretech

# MFA

Why

Pass the Hash

coretech

# How to configure MFA

- Why
- Services & Network to exclude
- Method
  - Call, Text, Azure Authenticator

coretech

# Demo

MFA

# Password reset

coretech

Is a password free

25% users forget their password on a regular basis


70% do not use a unique password for each website

Gartner estimate that 20%-50% of all service desk calls worldwide are for password reset

64% of users have written down their password at least once

33% WILL HAPPILY SHARE THEIR PASSWORD

coretech

# Demo

Password reset

coretech

# Active Directory Federation Services (ADFS)

coretech

# ADFS

Pros

- You control the authentication (no password sync to cloud). Single point of control
- 3rth party multifactor authentication solutions that can be integrated in ADFS. We have in Estonia MobileID or Estonian ID card that we can add there. This gives us ability to use Estonian gov ID.
- ADFS is not only SSO but also gives you:
  - Workplace Join
  - Work from anywhere – allows you to publish internal apps and services to external users

Cons

- Expensive
  - Load balancers, WAP servers, ADFS servers, 2 internet connections

# Identity in the cloud

Pros

- Simple, fast and easy and cheap
- Azure AD based Application Proxy
  - This allows as well to publish internal apps to external users without ADFS/WAP
- Better integration with SaaS etc?

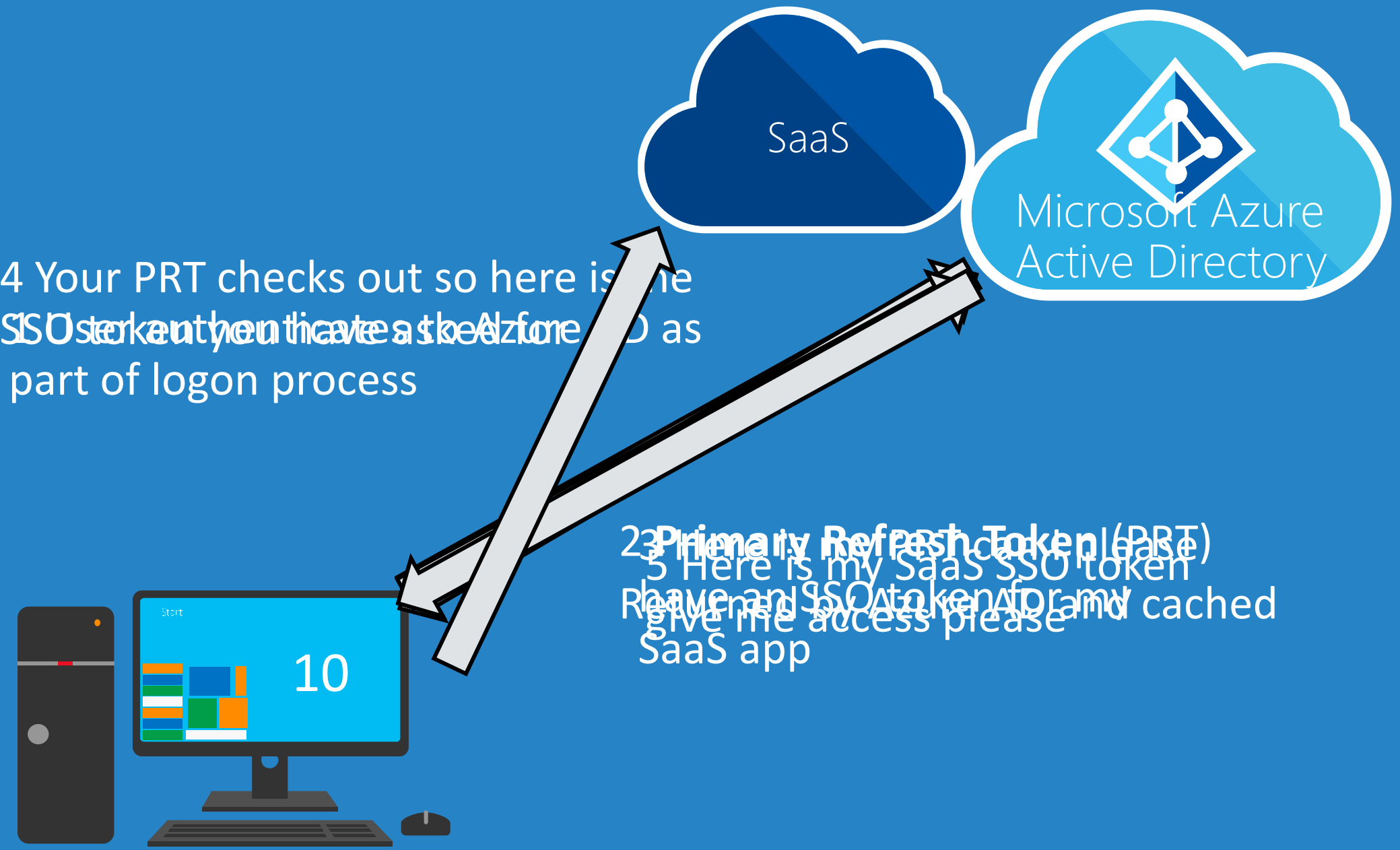
Cons

- Do you trust MS and MS based MFA?

coretech

# Software As a Service (SaaS)

# What happens behind the scenes



coretech

# Demo

## Software as a Service

coretech

# Azure Rights Management Service

coretech

# Secure and track

- Vision is to protect and share documents, files and emails anywhere with advanced tracking
- Templates
- Integration
  - SharePoint
  - Exhange online
  - On-prem

coretech

# Demo

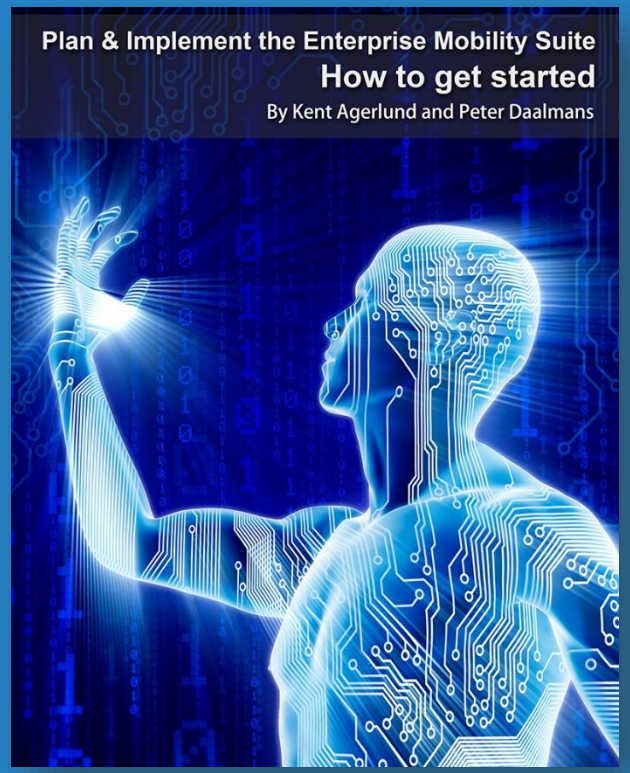
## Azure Rights Management

coretech

# Q/A + 15 Minute Break

Red dog is the code name for what?

Win, and we will ship you this book when it is published within a month!

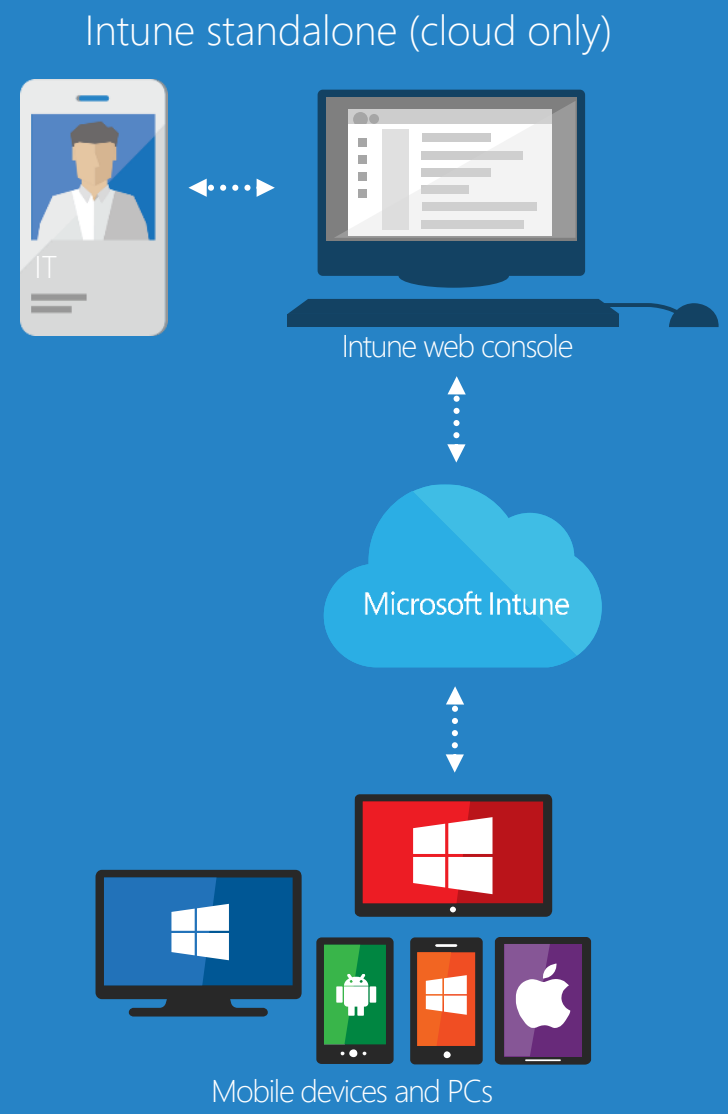


coretech

# Mobile Device Management: Infrastructure

# Deployment: Cloud Only

coretech




## Manage and Protect

- No existing infrastructure necessary
- No existing Configuration Manager deployment required
- Simplified policy control
- Simple web-based administration console
- Faster cadence of updates
- Always up-to-date

## Devices Supported

- Windows PCs (x86/64, Intel SoC)
- Windows RT
- Windows Phone 8.x/10.x
- iOS
- Android
- MAC OS X

# Deployment: Hybrid

coretech

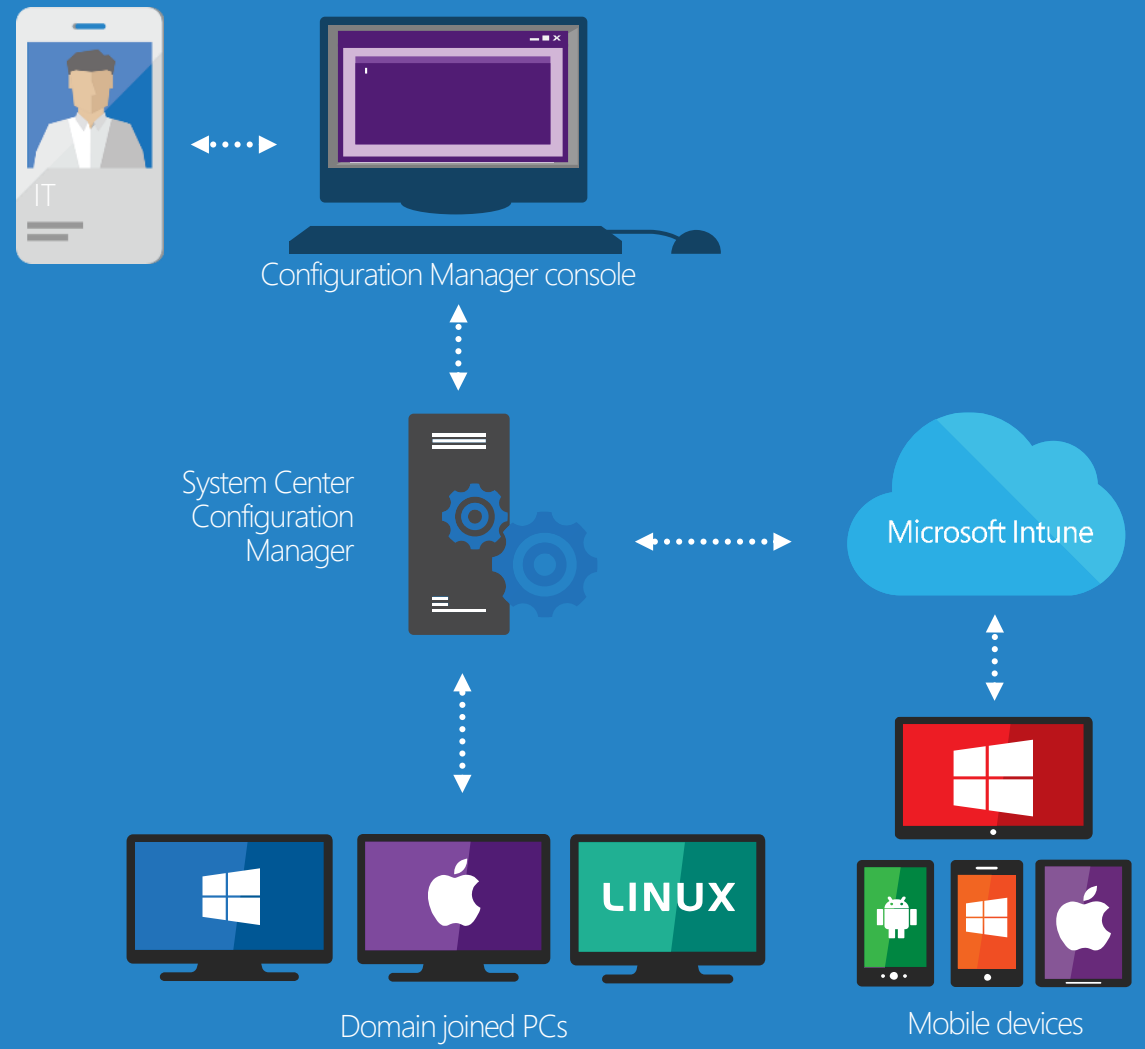
## System Center Configuration Manager with Microsoft Intune

- Build on existing Configuration Manager deployment
- Full PC management (OS deployment, endpoint protection, application delivery control, custom reporting)
- Deep policy control requirements
- Greater scalability
- Extensible administration tools (RBA, PowerShell, SQL reporting services)
- Automation
- Logging

## Devices Supported

- Windows PCs (x86/64, Intel SoC)
- Windows to Go
- Windows Server
- Linux
- Mac OS X
- Windows RT
- Windows Phone 8.x/10.x
- iOS
- Android

Configuration Manager integrated with Intune (hybrid)



# Comprehensive lifecycle management

## Enroll

- Provide a self-service Company Portal for users to enroll devices
- Deliver custom terms and conditions at enrollment
- Bulk enroll devices using Apple Configurator or service account
- Restrict access to Exchange email if a device is not enrolled

## Provision

- Deploy certificates, email, VPN, and WiFi profiles
- Deploy device security policy settings
- Install mandatory apps
- Deploy app restriction policies
- Deploy data protection policies


## Retire

- Revoke access to corporate resources
- Perform selective wipe
- Audit lost and stolen devices

## Manage and Protect

- Restrict access to corporate resources if policies are violated (e.g., jailbroken device)
- Protect corporate data by restricting actions such as copy/cut/paste/save outside of managed app ecosystem
- Report on device and app compliance

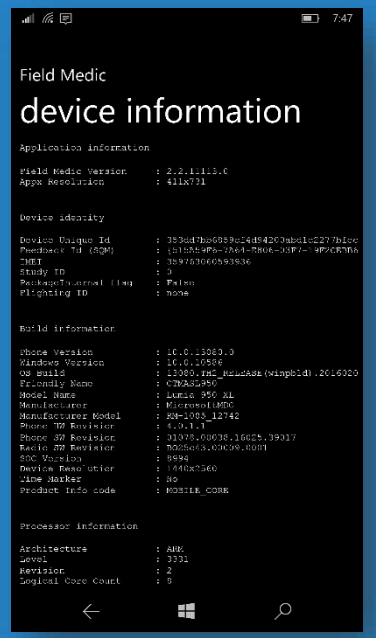
coretech

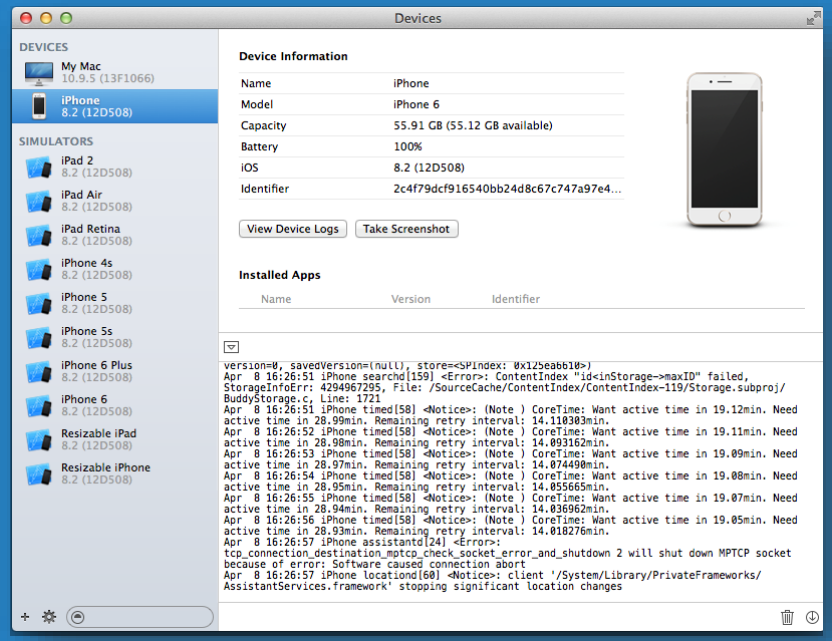
# Hybrid Requirements

- MDM Authority
- Intune connector
- UPN
- Collection

# Troubleshooting

- Android
  - <Device>\Phone\Android\data\com.microsoft.windowsintune.companyportal\files
  - 3 log files
- Windows Phone
  - Field Medic
- iOS
  - Get Xcode from the Appstore



coretech

# Demo

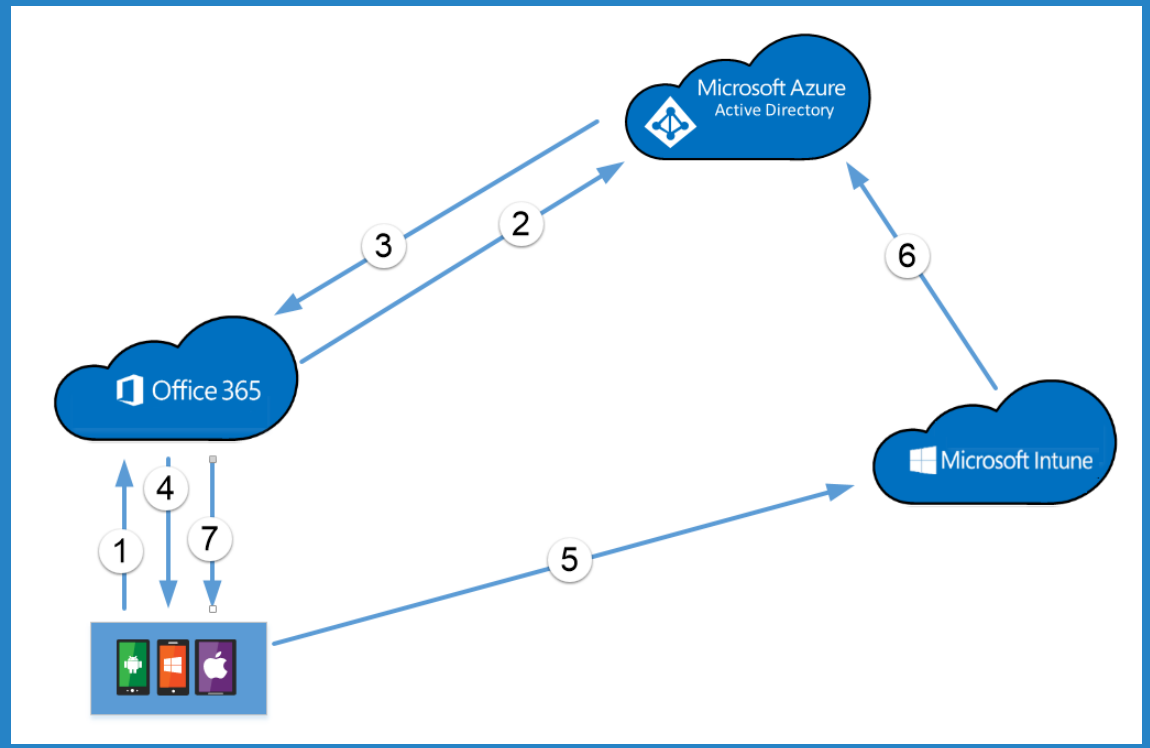
## Configure Infrastructure

coretech

# Security & Conditional Access

coretech

# Conditional Access




- User log on to the mobile device and configure email
- Office 365 checks with AAD to see if the device is managed and compliant.
- AAD returns the device state and in this case sees the device is not yet managed by Microsoft Intune.
- The device is placed into quarantine and the user receives a quarantine email

coretech

# Demo

## Conditional Access

coretech

# Application Management

coretech

# Applications

- Traditional Applications
- Store Apps and acceess
- Managed applications
- LOB applications
- Deny applications
- PowerShell

coretech

# Demo

## Application Management

coretech

# Resource Access

coretech

# Provide access to resources

- VPN
- WIFI
  - Certificate based
  - Password
    - Apple configurator
    - Existing Win10
    - http://johnathonb.com/2015/05/intune-android-pre-shared-key-generator

- Certificates

coretech

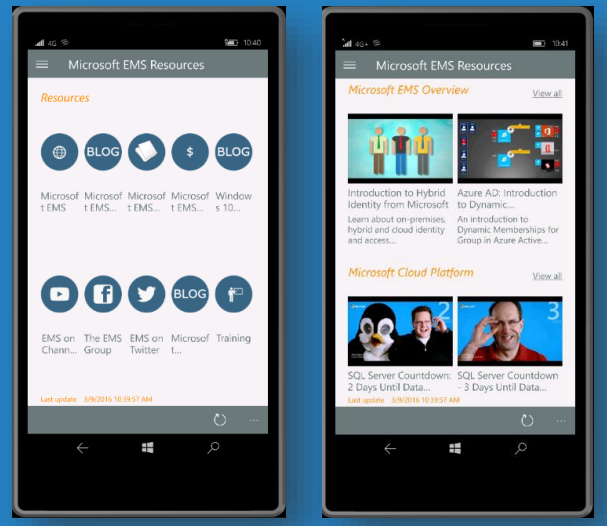
# Demo

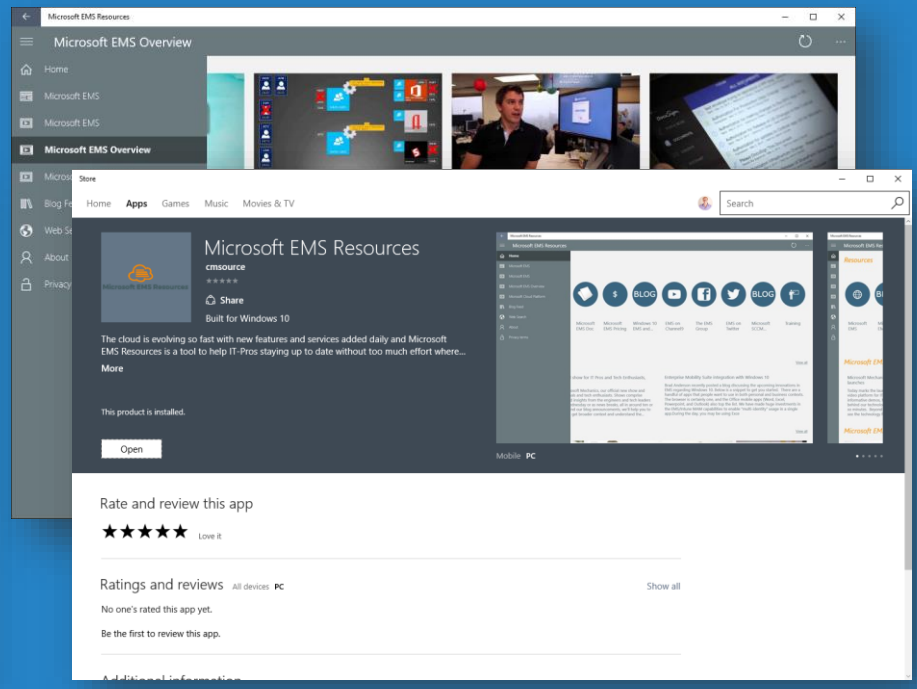
## Resource Access

# Enterprise Mobility Resources

In Store: Tilgjengelig til Windows 10 og Windows 10 Mobile

- https://www.microsoft.com/en-us/store/apps/microsoft-ems-resources/9nblggh6j3fq



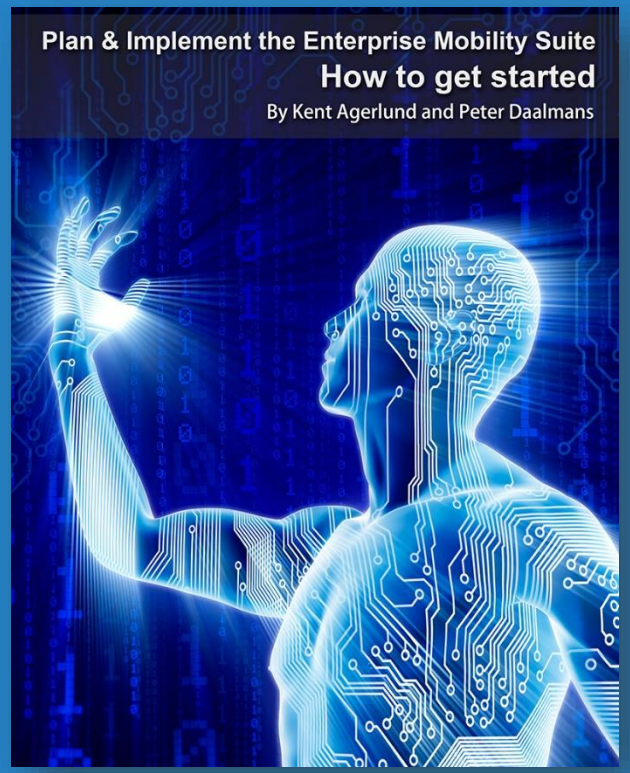



coretech

# Q/A

Red dog is the code name for what?

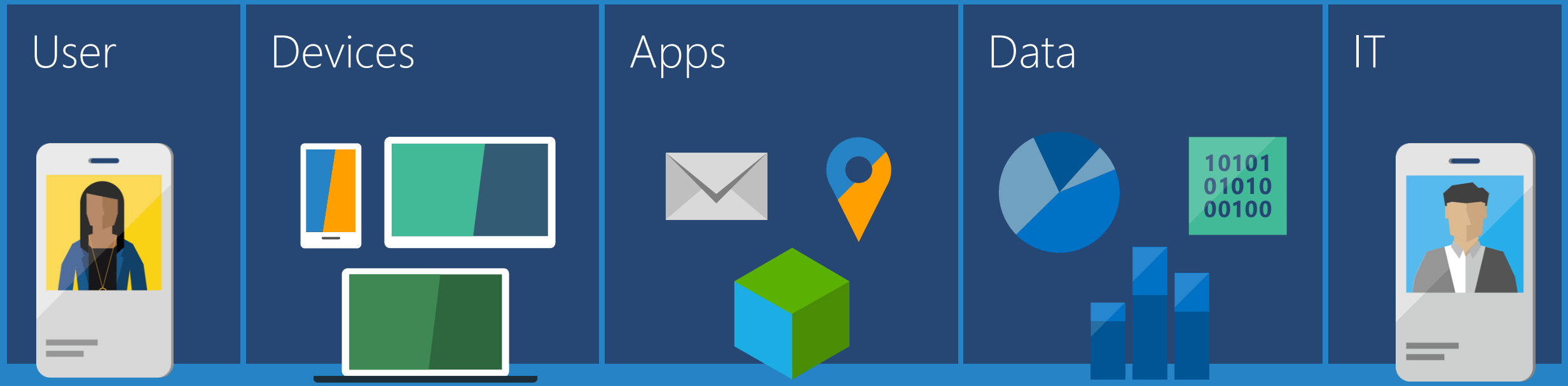
Win, and we will ship you this book when it is published within a month.



coretech

# Empowering enterprise mobility

People-centric approach




Enable your users

Unify your environment

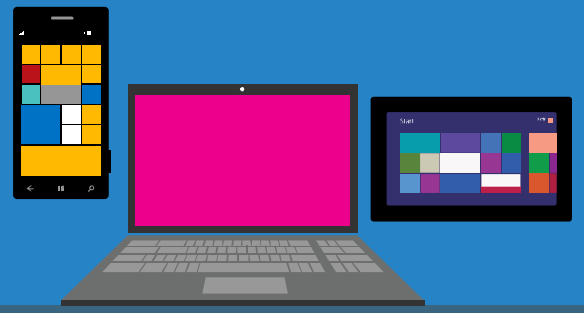
Protect your data

coretech

# Enterprise Mobility Suite (EMS)

## Not a single product, but several Cloud services

| Azure Active Directory Premium | Microsoft Intune | Azure Rights Management Service | Microsoft Advanced Threat Analytics |
|---|---|---|---|



coretech

# Thank you! =)