Herzlich Willkommen zum Microsoft IT Camp Windows 10 Enterprise Deployment

Eric Berg

Senior IT-Architekt - Microsoft Modern Workplace and Datacenter

Modern Workplace and Datacenter

Azure, System Center, Windows 10

Eric.Berg@comparex.de

@ericberg_de

http://ericberg.de/

COMPAREX
Software · Consulting · Services

MVP Microsoft® Most Valuable Professional

I'M SPEAKING!
GEEKSPRECH Podcast

Alexander Benoit

Senior Consultant / Head of Competence Center Microsoft

Arbeitsplatz der Zukunft

System Center Configuration Manager // Windows 10

Alexander.Benoit@sepago.de

@ITPirate

http://it-pirate.com/

sepago®

I'M SPEAKING!
GEEKSPRECH
Podcast

Microsoft IT Camps – Windows 10 Cyber Defense & Security

AGENDA

- Begrüßung, Vorstellung, Erwartungen
- Einführung Windows 10
- Neuer Ansatz Mobility
- Windows 10 Servicing
- Windows 10 Deployment
- Windows 10 Provisioning
- Weitere Tools

Microsoft IT Camps – Windows 10 Cyber Defense & Security

AGENDA

- Begrüßung, Vorstellung, Erwartungen
- Einführung Windows 10
- Neuer Ansatz Mobility
- Windows 10 Servicing
- Windows 10 Deployment
- Windows 10 Provisioning
- Weitere Tools

IT-Camps

www.entermo.de

Herzlich Willkommen zu den IT-Camps!

Wir freuen uns, dass du dabei bist!

In diesem ganztägigen Workshop fokussieren wir die wichtigsten N[illegible]ng-Features und Produkte innerhalb und rund um Windows 10. Dabei bearbeit[illegible] wir die beiden Schwerpunkte:

- Windows 10 Cyber Defense & Security
- Windows 10 Enterprise Deployment

in jeweils eigenen Tagesveranstaltungen.

Alle Infos zu den Inhalten beider [illegible]mps, Verlinkungen, Downloads etc. findest du auf dieser Seite. Solltest du dich für weitere IT-[illegible]mps interessieren – hier geht's zur Übersicht.

Du hast Fragen oder Feedback? Sprich uns bitte an, wir freuen uns! Alternativ kannst du dich auf den Feedback Bögen austoben.

Twittern

VERANSTALTUNGEN

Nov 18
Microsoft IT Camp Berlin – Windows 10 Cyber Defense & Security
9:00 - 17:00 - Berlin

Nov 25
Microsoft IT Camp Frankfurt – Windows 10 Enterprise Deployment
9:00 - 17:00 - Frankfurt

Nov 22
Microsoft IT Camp Köln – Windows 10 Enterprise Deployment
9:00 - 17:00 - Köln

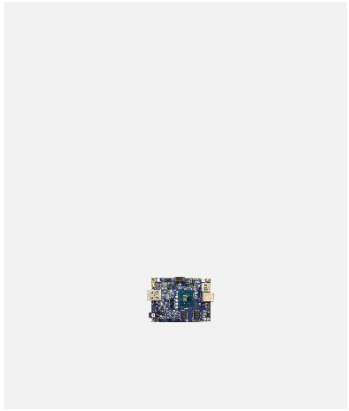
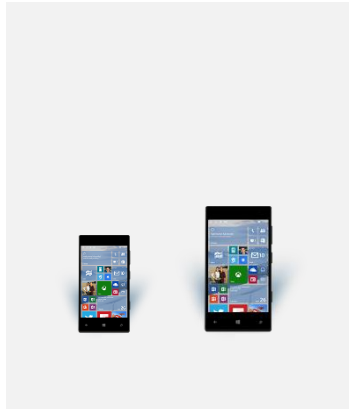
Nov 14
Microsoft IT Camp München – Windows 10 Cyber Defense & Security
9:00 - 17:00 - München

Devise des Tages:

Microsoft IT Camps – Windows 10 Cyber Defense & Security

AGENDA

- Begrüßung, Vorstellung, Erwartungen
- Einführung Windows 10
- Neuer Ansatz Mobility
- Windows 10 Servicing
- Windows 10 Deployment
- Windows 10 Provisioning
- Weitere Tools



One converged **Windows** platform

2001

Windows XP

- Logon (Ctrl+Alt+Del)
- Access Control
- User Profiles
- Security Policy
- Encrypting File System (File Based)
- Smartcard and PKI Support
- Windows Update

2004

Windows XP SP2

- Address Space Layout Randomization (ASLR)
- Data Execution Prevention (DEP)
- Security Development Lifecycle (SDL)
- Auto Update on by Default
- Firewall on by Default
- Windows Security Center
- WPA Support

2007

Windows Vista

- Bitlocker
- Patchguard
- Improved ASLR and DEP
- Full SDL
- User Account Control
- Internet Explorer Smart Screen Filter
- Digital Right Management
- Firewall improvements
- Signed Device Driver Requirements
- TPM Support
- Windows Integrity Levels
- Secure “by default” configuration (Windows features and IE)

2009

Windows 7

- Improved ASLR and DEP
- Full SDL
- Improved IPSec stack
- Managed Service Accounts
- Improved User Account Control
- Enhanced Auditing
- Internet Explorer Smart Screen Filter
- AppLocker
- BitLocker to Go
- Windows Biometric Service
- Windows Action Center
- Windows Defender

2012

Windows 8

- Firmware Based TPM
- UEFI (Secure Boot)
- Trusted Boot (w/ELAM)
- Measured Boot
- Significant Improvements to ASLR and DEP
- AppContainer
- Windows Store
- Internet Explorer 10 (Plugin-less and Enhanced Protected Modes)
- Application Reputation moved into Core OS
- Device Encryption (All SKU)
- BitLocker improvements and MBAM
- Virtual Smartcards
- Dynamic Access Control
- Built-in AV (Windows Defender)
- Improved Biometrics
- TPM Key Protection and Attestation
- Certificate Reputation
- Provable PC Health
- Remote Business Data Removable

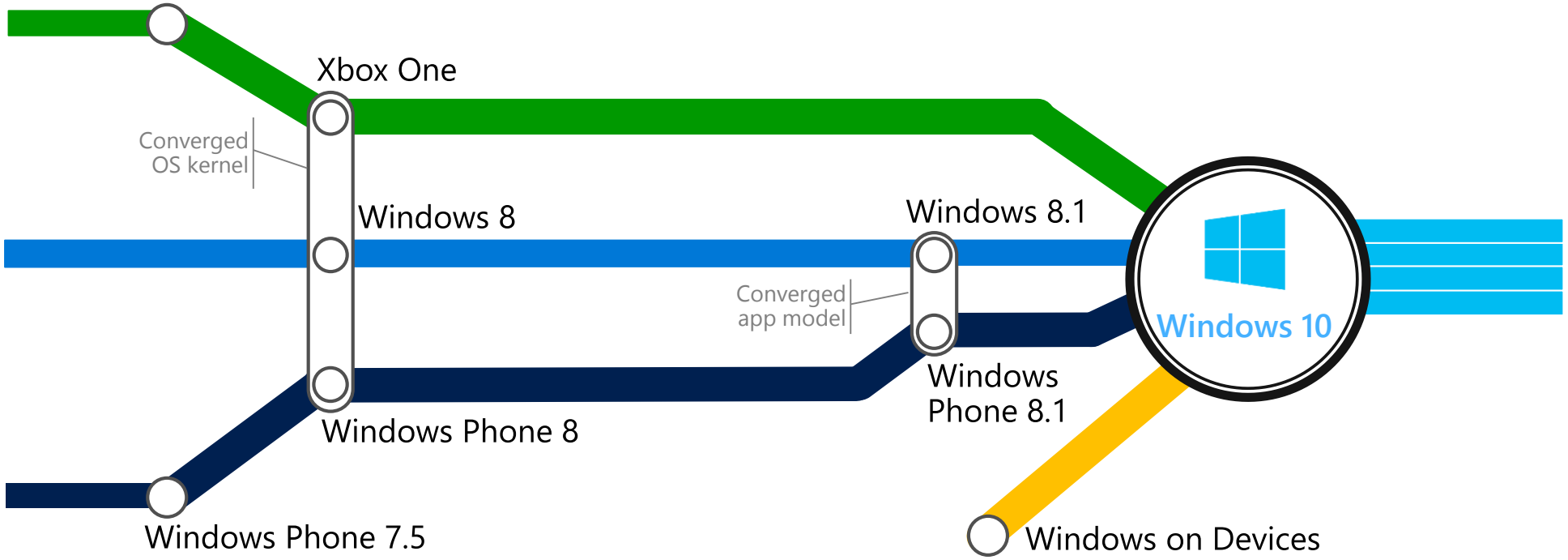
2015

Windows 10

- Virtual Secure Mode
- Virtual TPM
- Control Flow Guard
- Microsoft Passport
- Windows Hello
- Biometric Framework Improvements (Iris, Facial)
- Broad OEM support for Biometric enabled devices
- Enterprise Data Protection
- Device Encryption supported on broader range of devices
- DMA Attack Mitigations
- Device Guard
- URL Reputation Improvements
- App Reputation Improvements
- Windows Defender Improvements
- Provable PC Health Improvements

Convergence

Journey to Convergence



Microsoft IT Camps – Windows 10 Cyber Defense & Security

AGENDA

- Begrüßung, Vorstellung, Erwartungen
- Einführung Windows 10
- Neuer Ansatz Mobility
- Windows 10 Servicing
- Windows 10 Deployment
- Windows 10 Provisioning
- Weitere Tools

Management Choices

Traditional Management

- Works with existing infrastructure
- Continued support for Group Policy and WMI

Modern Management

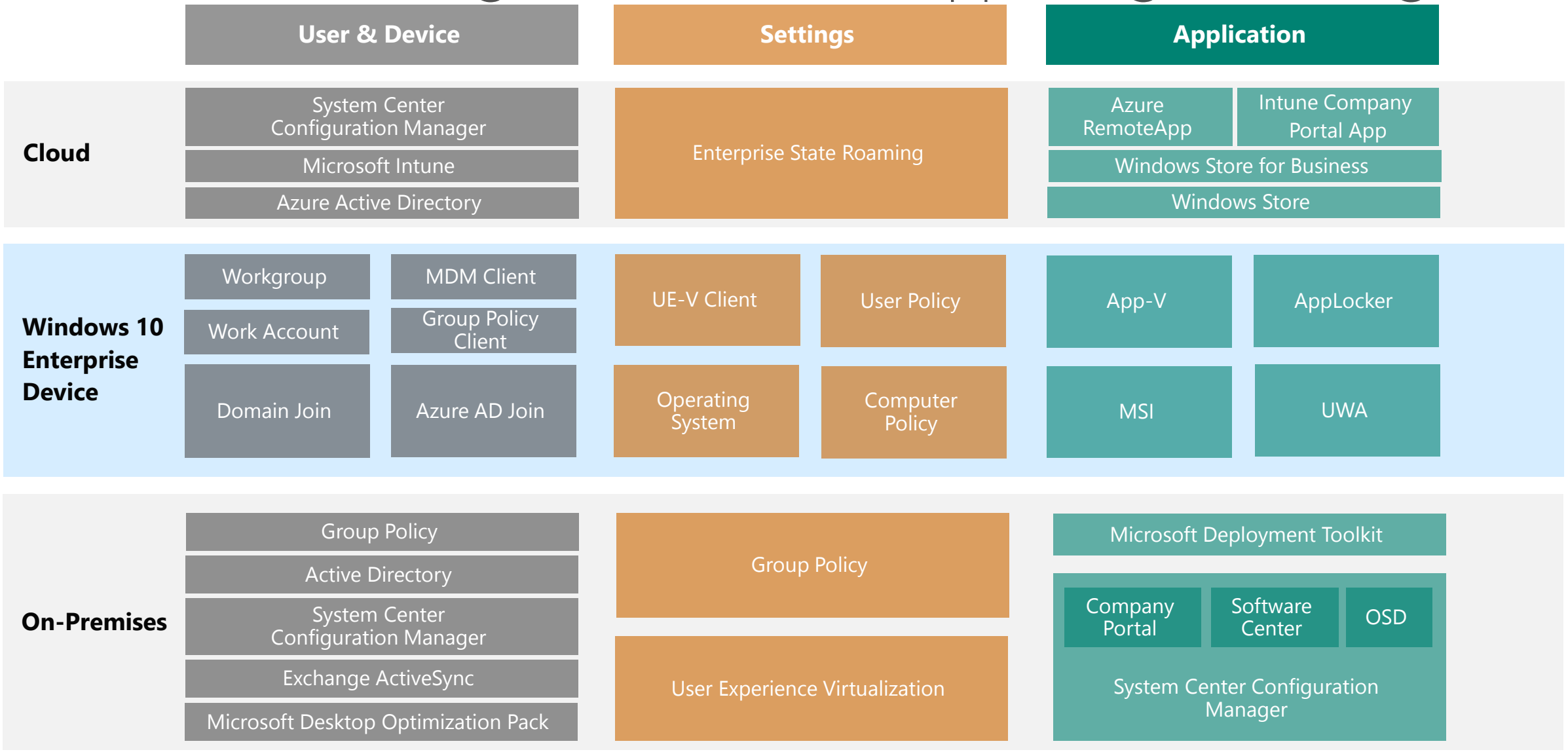
- Advanced MDM support
- Consistent across PC/phone
- 1st and 3rd party solutions

Available Choices	
Identity	▪ Active Directory ▪ Azure Active Directory
Management	▪ Group Policy ▪ System Center Configuration Manager ▪ 3rd Party Infrastructure Management ▪ Microsoft Intune ▪ 3rd Party MDM
Updates & Upgrades	▪ Windows Update ▪ Windows Server Update Services ▪ Software Update Point (System Center Configuration Manager) ▪ Microsoft Intune ▪ 3rd Party MDM
Infrastructure	▪ On Premises ▪ Cloud
Ownership	▪ Corporate Owned ▪ Choose Your Own Device ▪ Bring Your Own Device

Management Capability & Scenario Matrix

	Capabilities	Scenarios			
		Evergreen Windows 10 management	Take control of mobile devices	Familiar user experience	Reduce device onboarding costs
User & Device	Traditional Management	✓	✘	✓	✘
	Modern Management	✓	✓	✓	✘
	Provisioning	✘	✘	✘	✓
Settings	Policy Configuration	✓	✓	✓	✓
	OS Customization	✘	✓	✓	✘
	Enterprise State Roaming	✘	✘	✓	✘
	On-Premises Roaming	✘	✘	✓	✘
Applications	Device Targeted	✘	✘	✓	✘
	User Targeted	✘	✘	✓	✘
	Self Service	✘	✘	✓	✓

Windows 10 Management Stack & Supporting Technologies

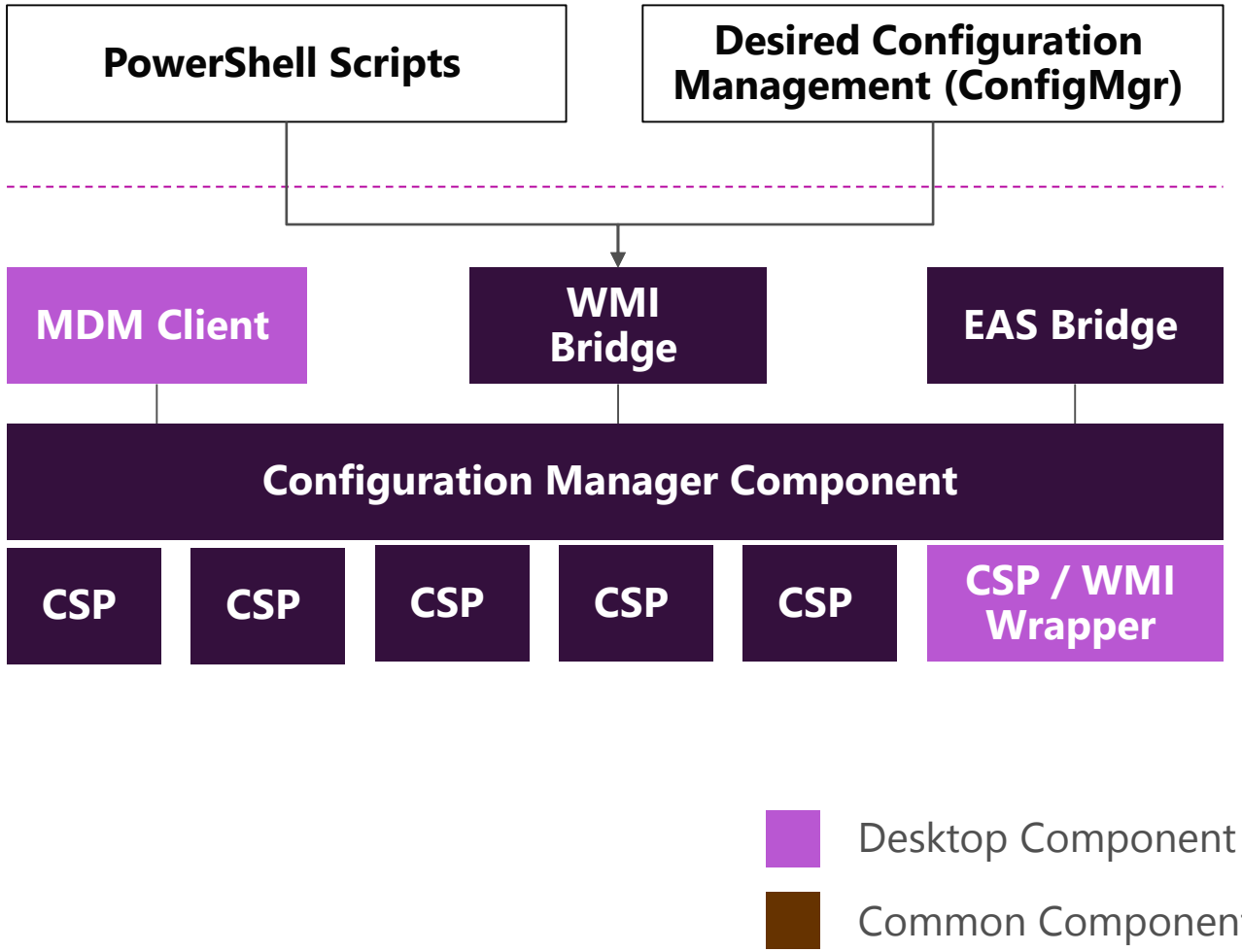


Management Architecture

- Alternative method to Group Policy management.
- Companies may use both approaches to manage devices .

- MDM client on Windows 10 talks through Configuration Manager component (not System Center) to other components including Configuration Service Providers (CSP) for additional MDM features / functionality

- WMI Bridge exposes MDM settings available, which administrators can be configured via DCM (ConfigMgr) or PowerShell



System Center Configuration Manager

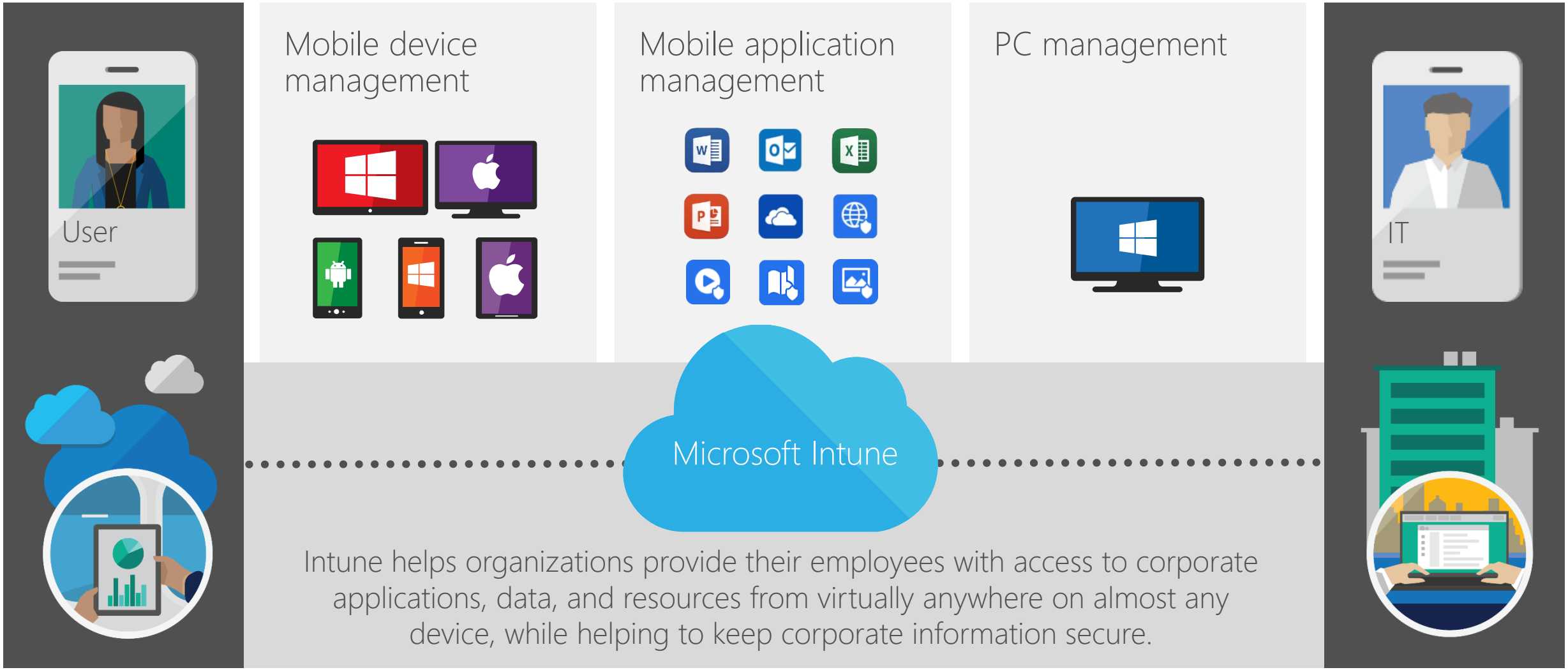
Lifecycle

Product version	Release vehicle	Availability	Features supported	Support	Windows Servicing Model supported
System Center Configuration Manager	**Current Branch**	December 2015 with updates released periodically throughout the year	New features, security updates, bug fixes	Can defer updates for up to 12 months before you must deploy updates to maintain support	Windows 10 Current Branch, Current Branch for Business, and Long Term Servicing Branch

Management Support for Windows 10

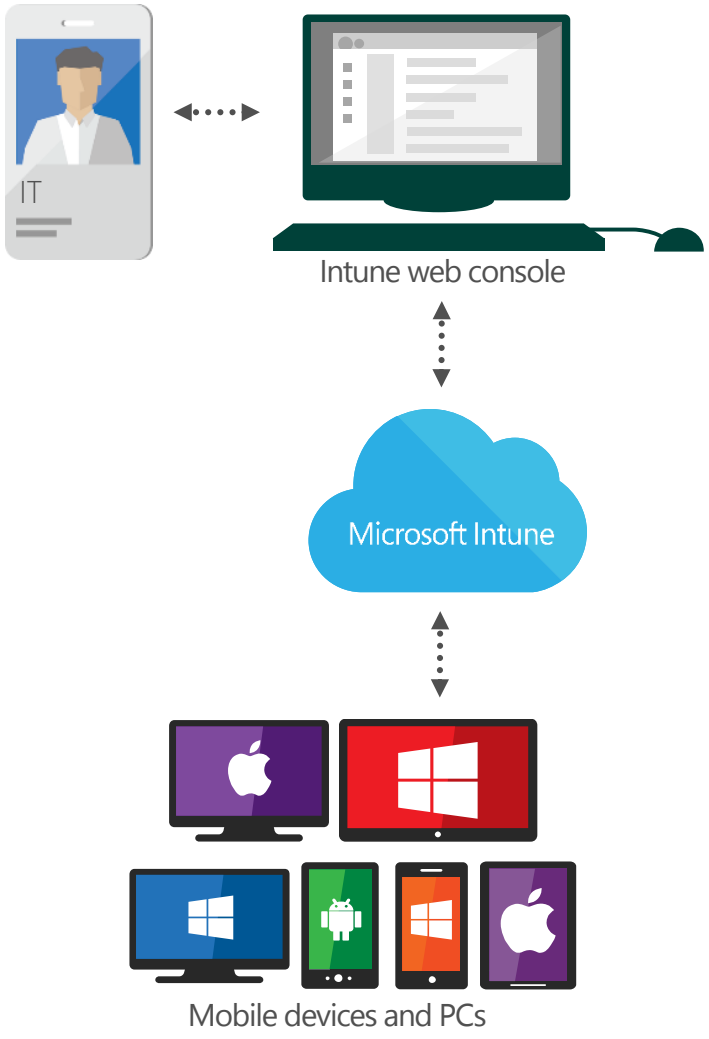
System Center Configuration Manager Version		Windows 10 Version			
		LTSB 2015	1507	1511	1607
2007		Management Only			
2012 SP2 or R2 SP1					
Current Branch	1511				
	1602				App Compat of Current Branch
	1606				

Modern Management with Microsoft Intune

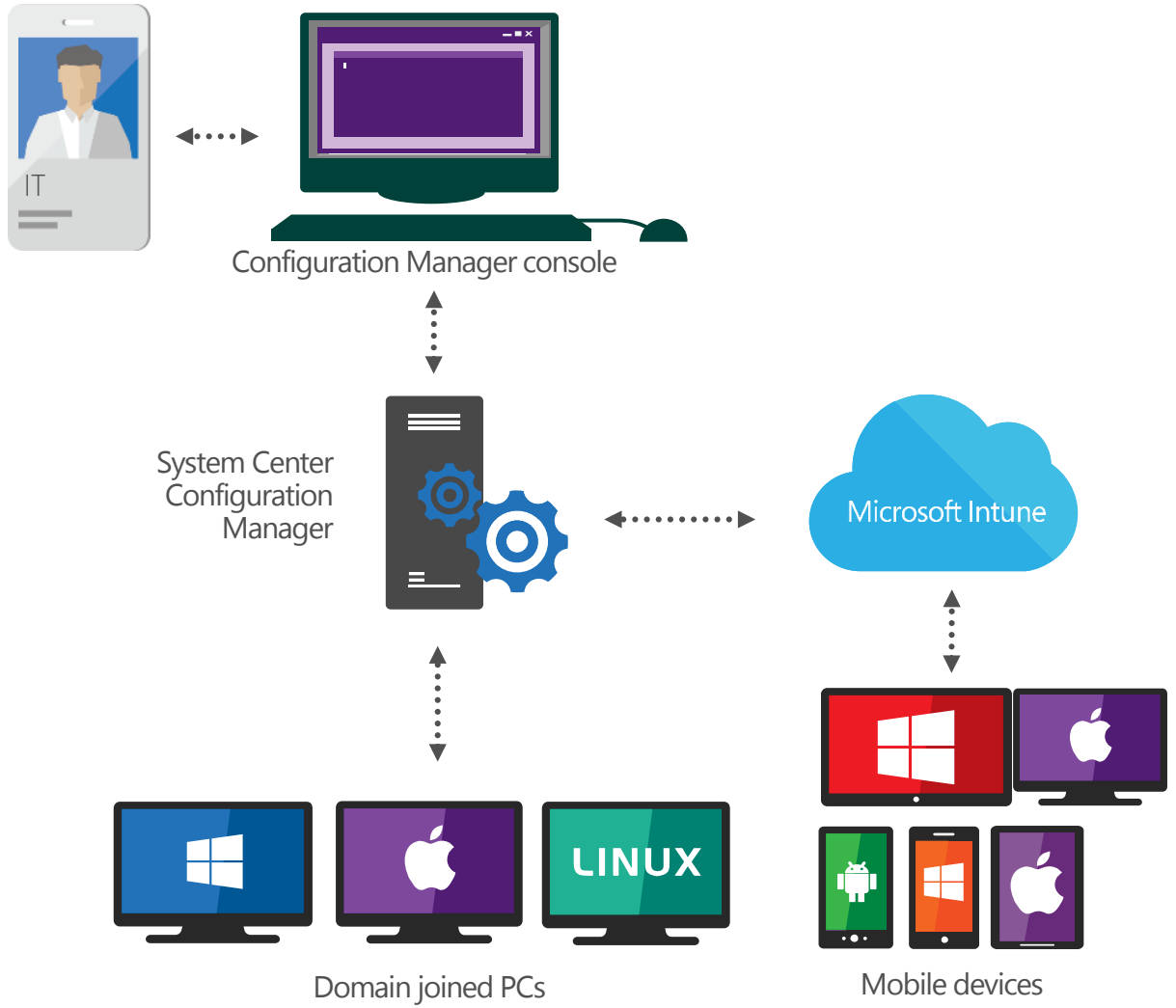


Microsoft Intune Deployment Flexibility

Intune standalone (cloud only)



Configuration Manager integrated with Intune (hybrid)



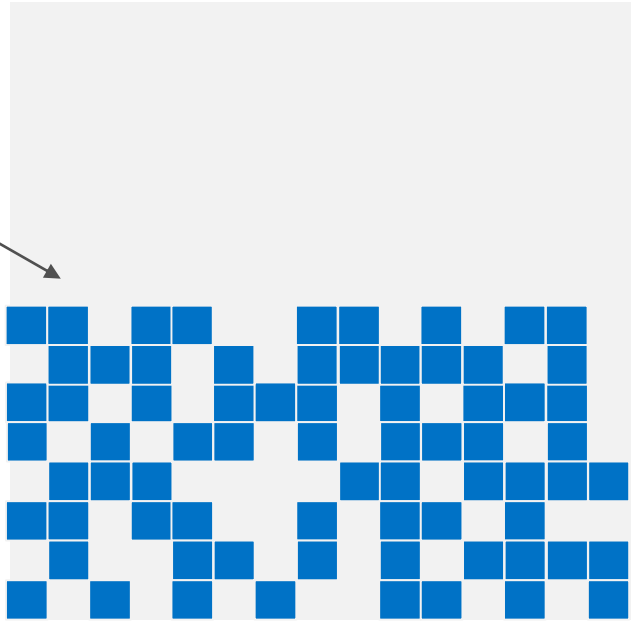
Microsoft IT Camps – Windows 10 Cyber Defense & Security

AGENDA

- Begrüßung, Vorstellung, Erwartungen
- Einführung Windows 10
- Neuer Ansatz Mobility
- Windows 10 Servicing
- Windows 10 Deployment
- Windows 10 Provisioning
- Weitere Tools

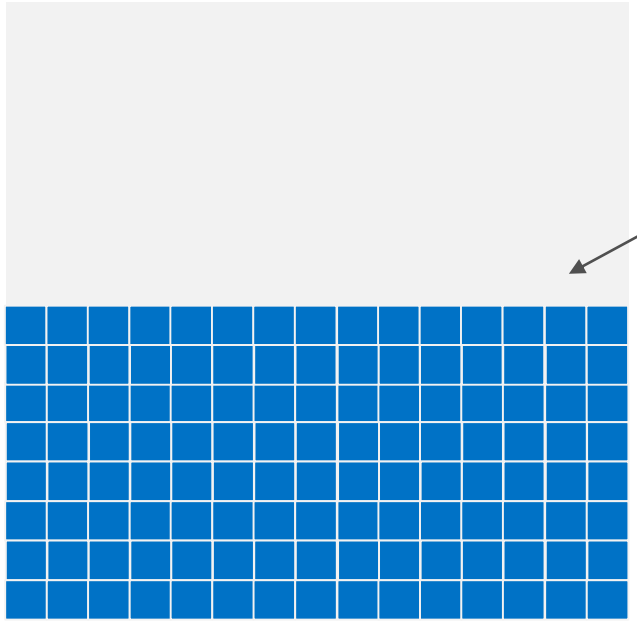
Traditional Enterprise Servicing of Windows

What customers are running



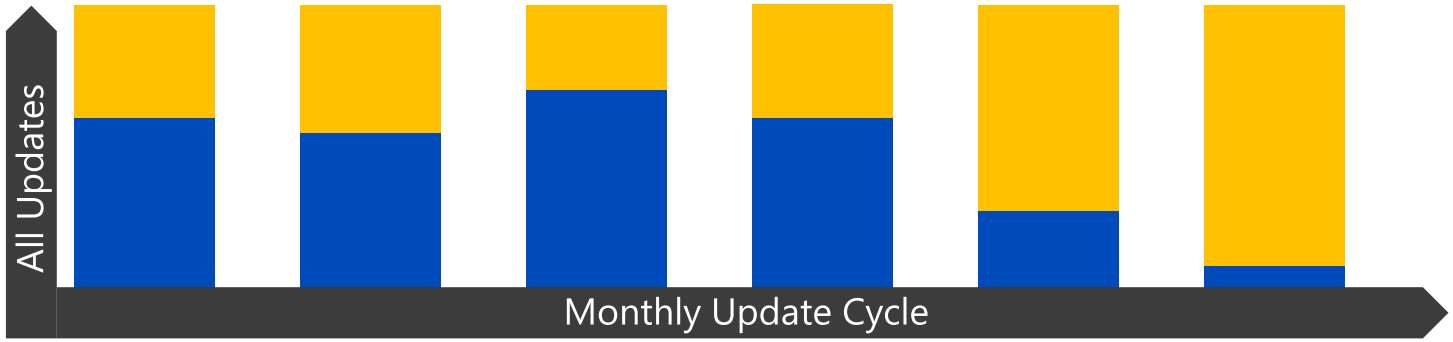
Typical Windows 7 PC:
Selectively Patched

What Microsoft is testing



Windows 7 Test Lab PC:
Fully Patched

Traditional Enterprise Servicing of Windows



Microsoft Update Release

- Monthly update release ("Patch Tuesday")
- Innovation delivered at Service Pack
- Long service pack release cycle
- Long vNext cycle

Corporate Deployment

- Selective deployment of updates
- Selectivity justified by AppCompat, bandwidth, others
- App remediation typically "shelved" and updates never applied

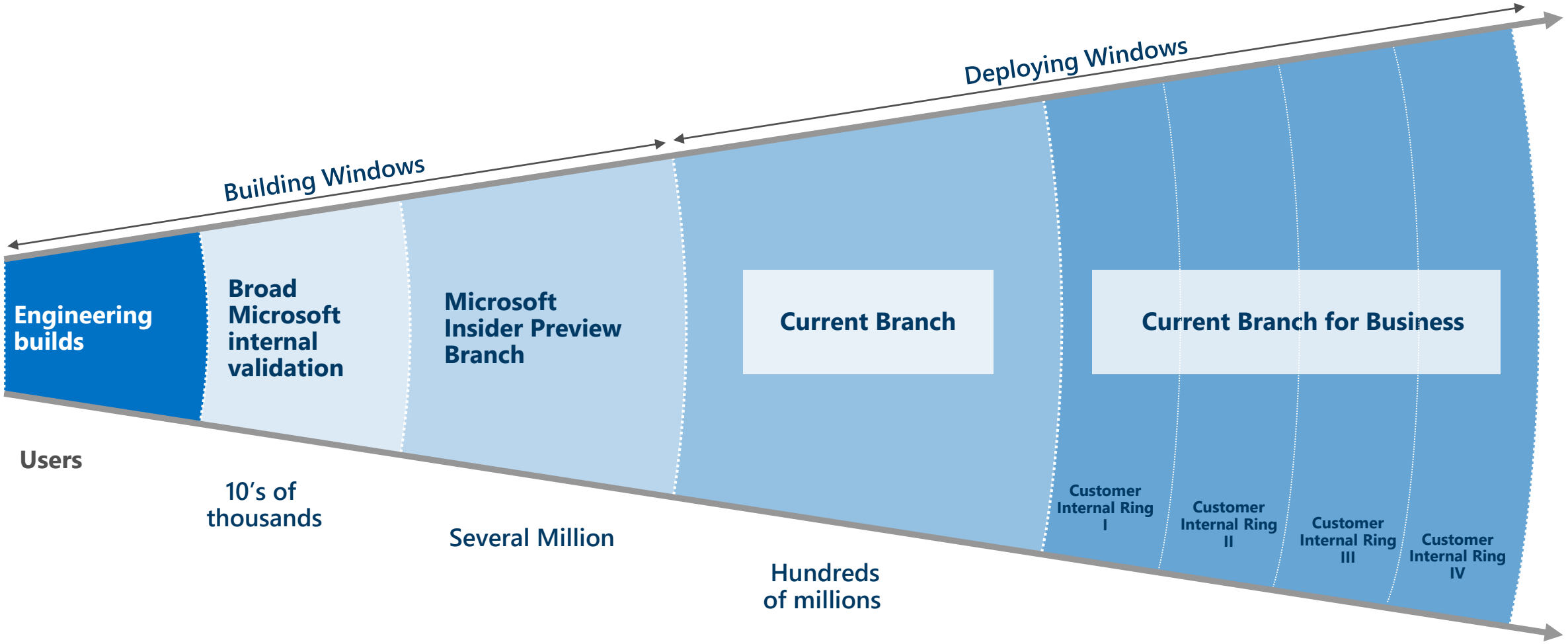
Update and Innovation Gap

- Accepted short-term risk increase
- Insidious long-term risk
- App portfolio ages
- Out-dated system baselines
- Costly to operate non-homogenous estate
- Hidden remediation cost - "remediate" before an upgrade

Understanding WaaS through Scenarios

	Capabilities	Scenarios			
		Evergreen platform	Protect mission critical systems	Control Windows adoption	Keep devices updated
Branches	Windows Insider Preview	✓	✗	✗	✓
	Current Branch	✓	✗	✓	✓
	Current Branch for Business	✓	✗	✓	✓
	Long Term Servicing Branch	✗	✓	✓	✓
Operate	Defer Feature Updates	✗	✓	✓	✓
	Move Branches	✗	✓	✓	✓
Integrate	Cloud Update Delivery	✓	✗	✗	✓
	On-Prem Update Delivery	✓	✓	✓	✓
Plan	Service Management	✓	✓	✓	✓

Windows as a Service Branches



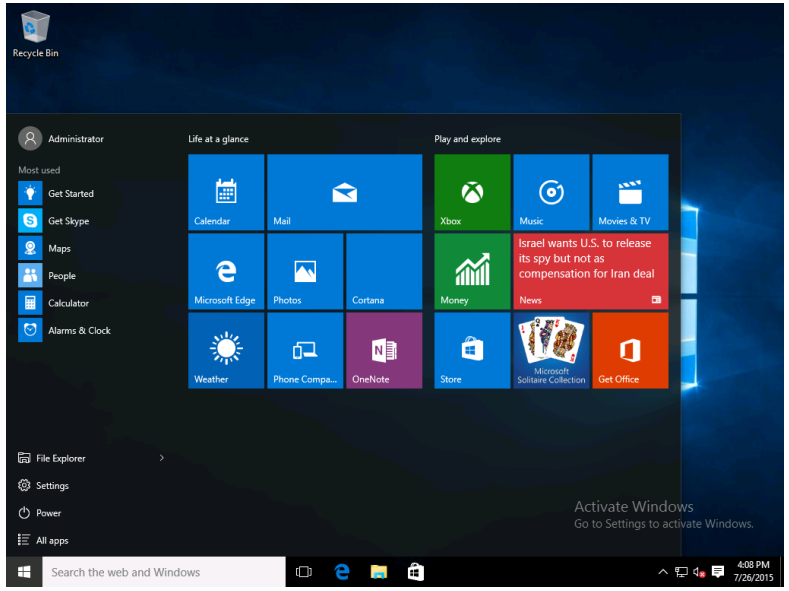
*Conceptual illustration only

Current Branch for Business vs. Long Term Servicing Branch

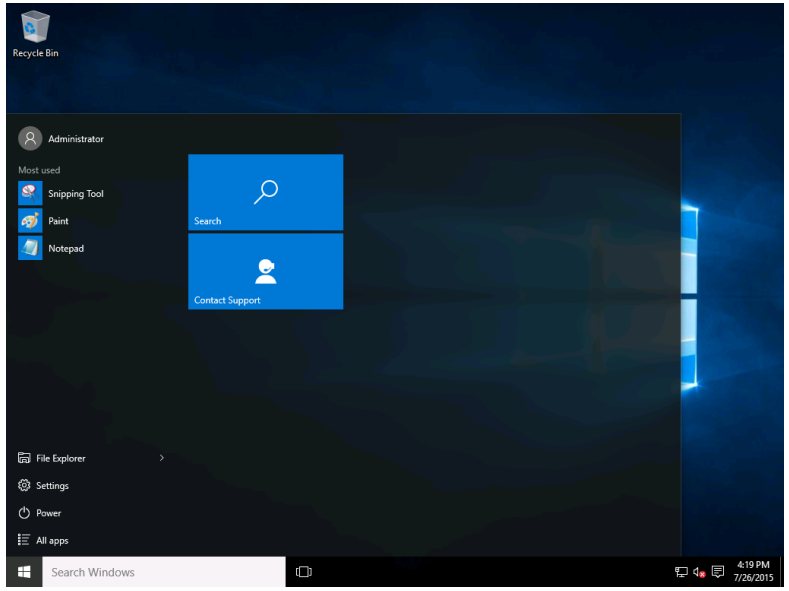
Capabilities	Current Branch for Business (CBB)	Long Term Servicing Branch (LTSB)
Recommended Enterprise use scenario	General information worker systems; salesforce, etc.	Special systems: Air Traffic Control; Hospital ER, etc.
Value of the latest features as they are released	✓	
Several months to consume feature updates	✓	
1st party browsing choices	Microsoft Edge, IE 11	IE 11
Support for Universal Office and some 1st party Universal apps	✓	
Support for Win 32 Office	✓	✓
Ongoing security updates for the lifetime of the branch	✓	✓
Ability to load universal apps	✓	✓
No feature upgrade required to stay supported		✓

Current Branch for Business vs. Long Term Servicing Branch

Capabilities	Current Branch for Business (CBB)	Long Term Servicing Branch (LTSB)
Transform Pro to Enterprise	✓	
Bulk Upgrade from WU	Pro only	
Bulk upgrade using media	✓	✓

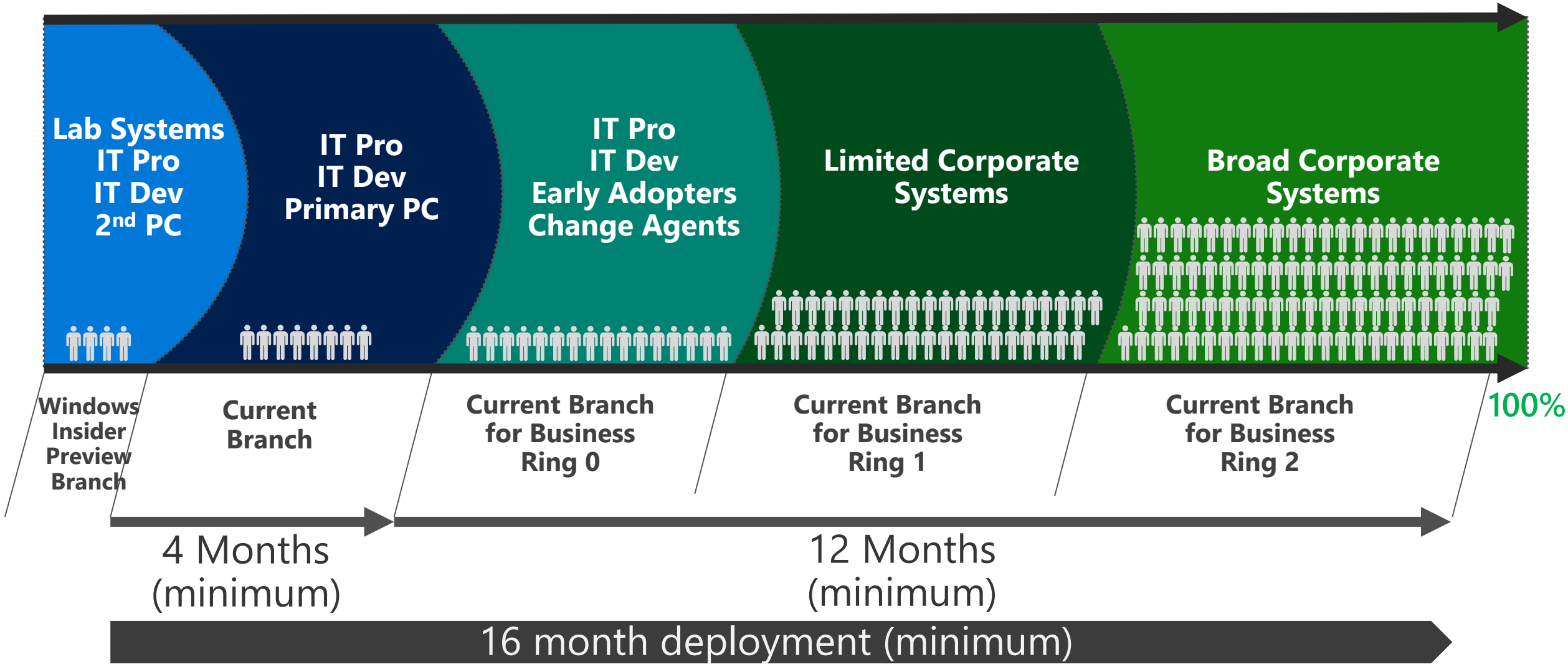


Microsoft Windows 10 Enterprise

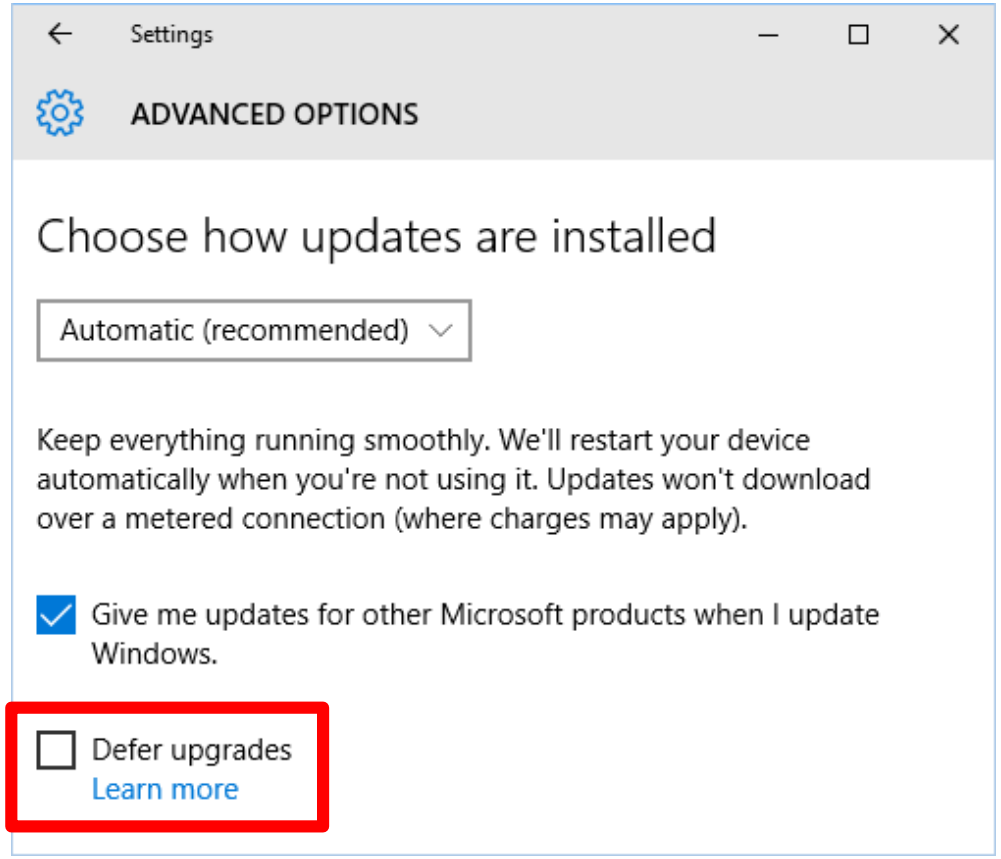


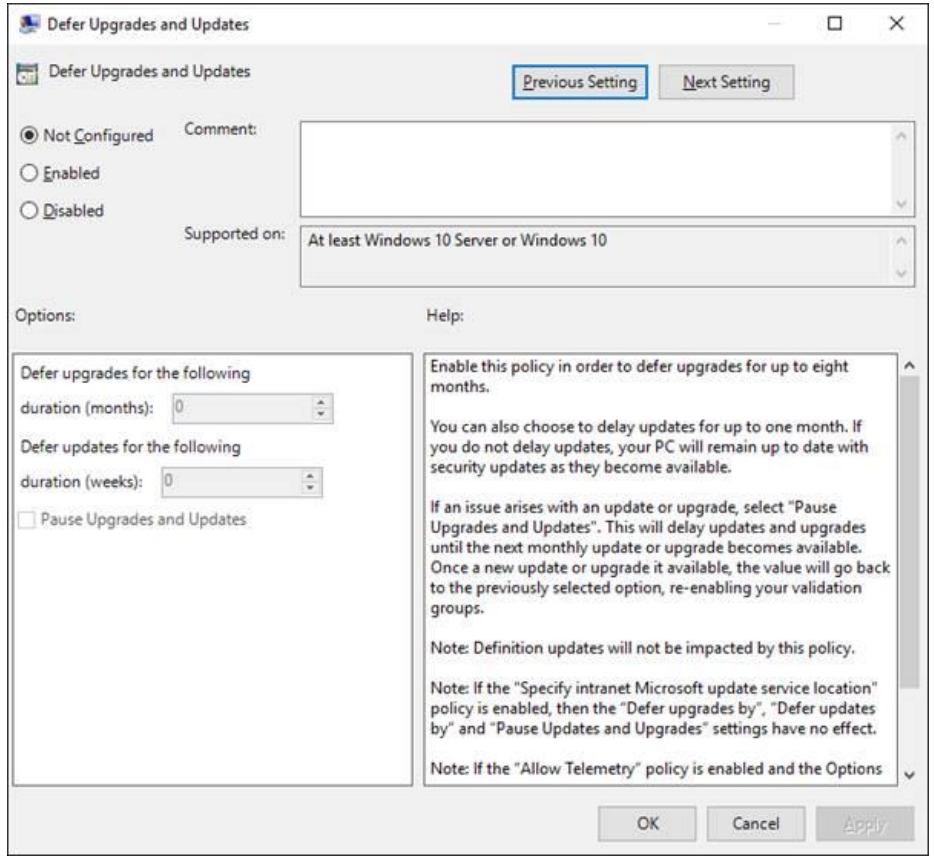
Microsoft Windows 10 Enterprise 2015 LTSB

Adoption Planning



Implement with Windows Update for Business

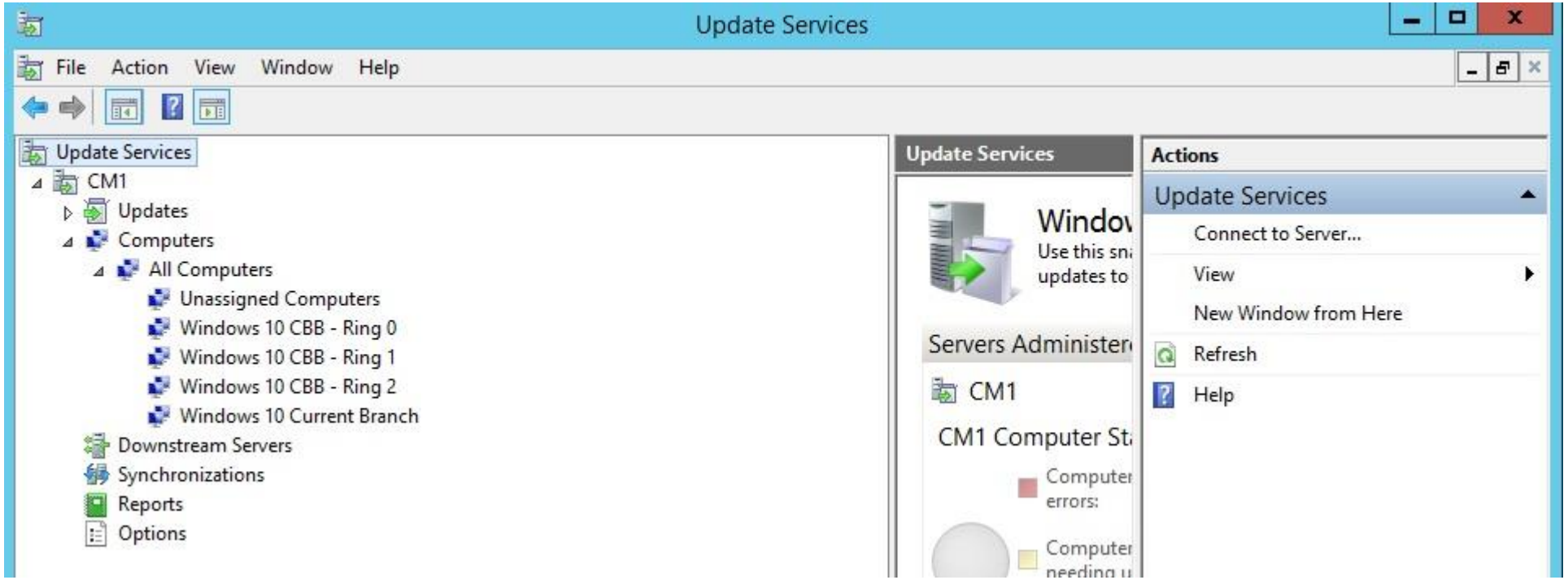




Computer Configuration -> Administrative Templates -> Windows Components -> Windows Update

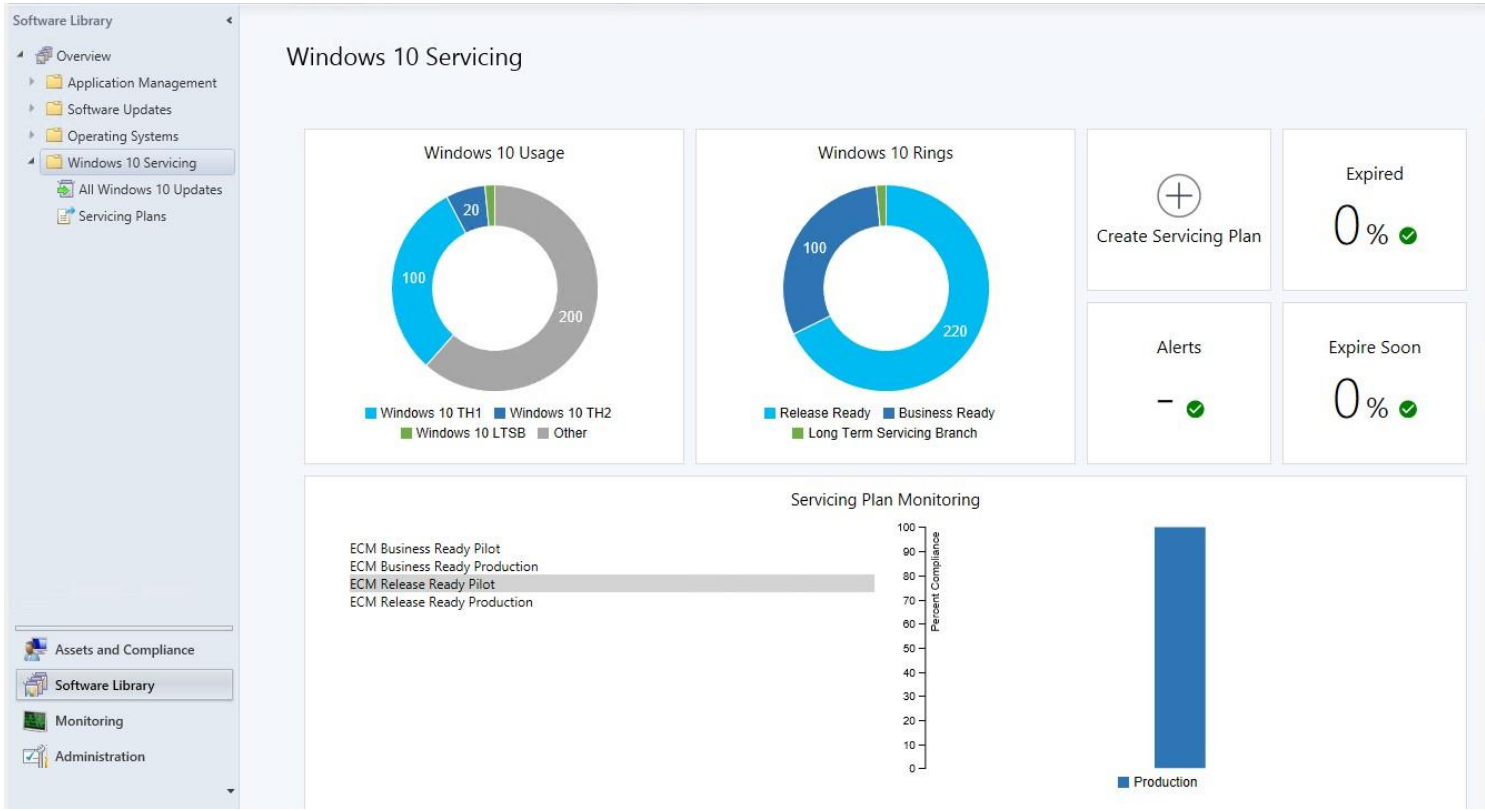
This setting configures Windows Update. WSUS and Configuration Manager settings are not impacted.

Implement with Windows Server Update Services



1. Create Computer Groups to match ring structure
2. Add devices to groups
3. Approve and assign quality and feature updates / to groups

Implement with System Center Configuration Manager



1. View the state of Windows 10 in the environment
2. Create a Windows 10 servicing plan
3. Deploy Windows 10 servicing content to devices

Microsoft IT Camps – Windows 10 Cyber Defense & Security

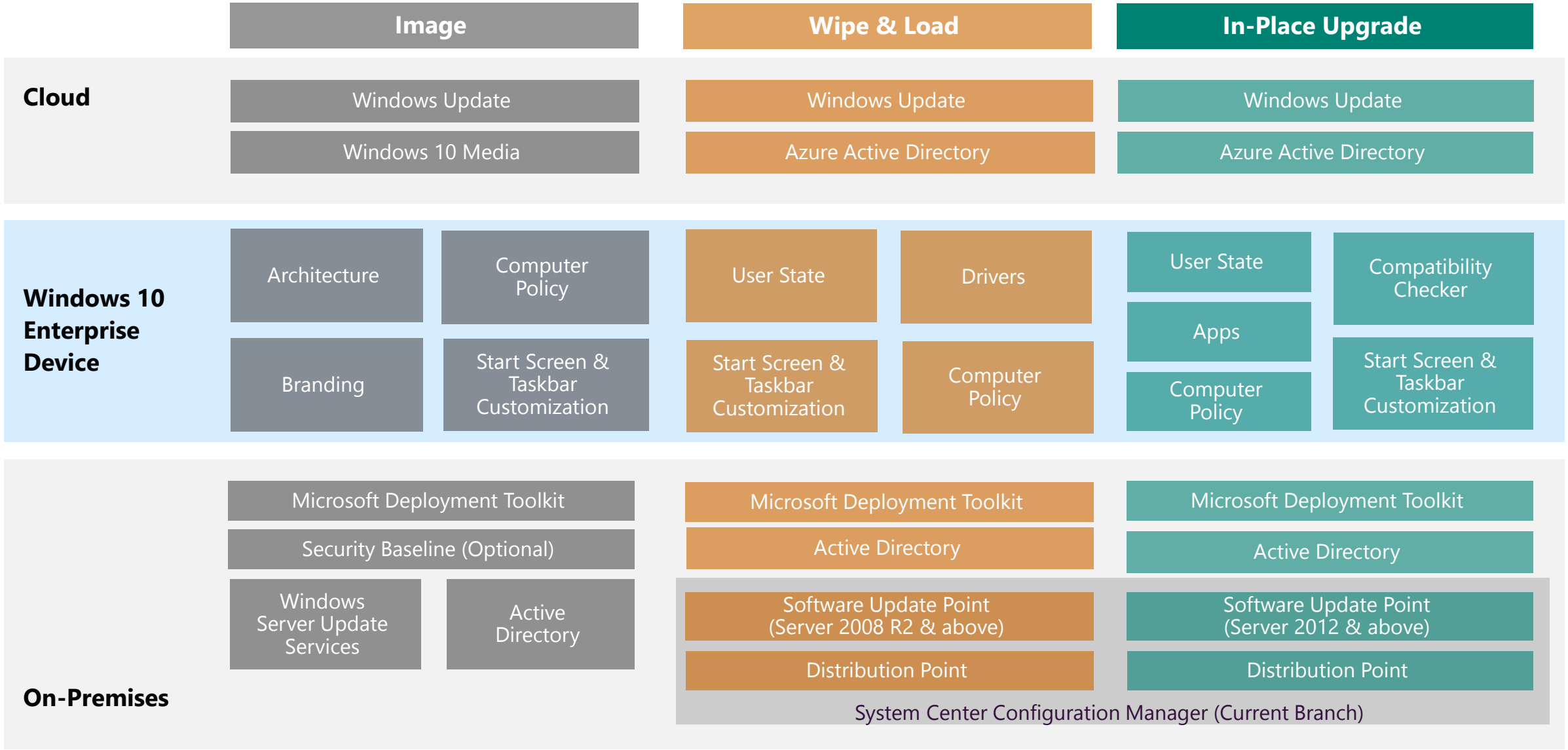
AGENDA

- Begrüßung, Vorstellung, Erwartungen
- Einführung Windows 10
- Neuer Ansatz Mobility
- Windows 10 Servicing
- Windows 10 Deployment
- Windows 10 Provisioning
- Weitere Tools

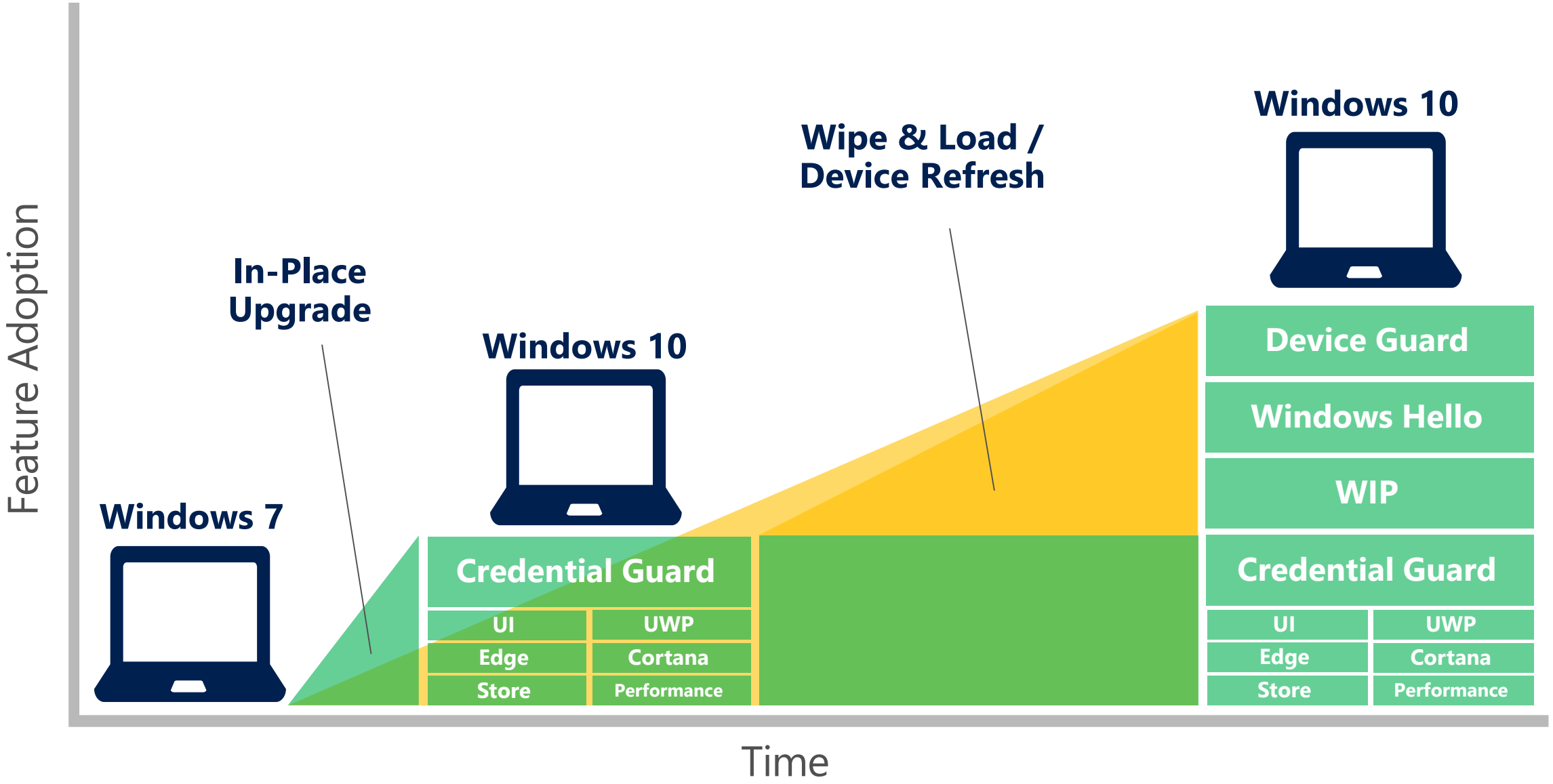
Deployment capability and scenario matrix

	Capabilities	Scenarios		
		Pilot Windows 10	Scale Deployment	Retain Apps & Settings
Image Creation	Vanilla Image	✓	✓	✘
	Customized Image	Optional	✓	✓
Wipe & Load	New Device	Optional	✓	✘
	Replace Device	Optional	Optional	✓
	Refresh Device	✓	✓	✓
In-Place Upgrade	Upgrade OS	✓	✓	✓

Windows 10 Deployment Stack & Supporting Technologies



Transformation Choices



Deploying Windows 10

New Device

Bare Metal
(Custom Image)

Existing Device

Device Considerations

- BIOS → UEFI
- Disk partitioning
- WinPE Offline Operation
- 3rd party disk encryption*

Operating System Considerations

- Architecture (x86 → x64)
- Base OS language
- Domain
- Local Administrators
- Configuration drift
- Moving from XP or Vista
- Custom base image

Application Considerations

- Bulk app change

In-Place Upgrade

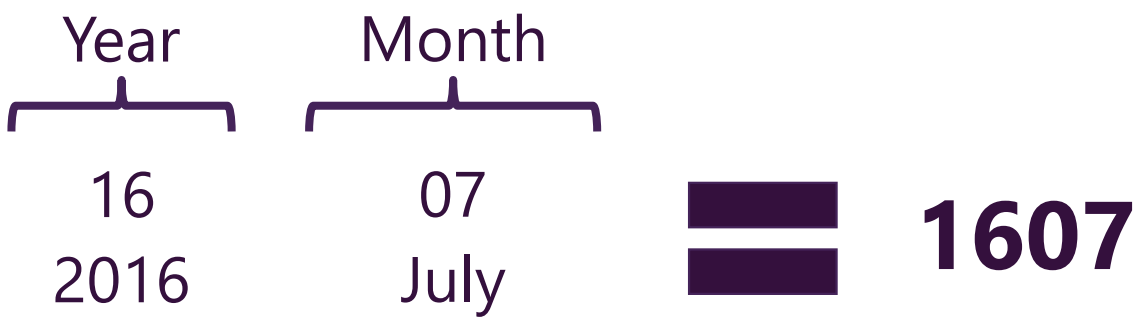
Upgrade key apps as needed post OS update

Refresh (Wipe & Load)
Re-install the operating system (Custom Image)
Install applications
Migrate user state

Windows version reference

Version	Availability date	Latest revision date
1507	July 2015	March 2016
1511	November 2015	March 2016
1607	August 2016	August 2016

Version number is build complete date:



Availability date:
Date of the initial public release of the version

Latest revision date:
Release date of the most recent update to the version

Windows Tooling & Deployment Capabilities

Overview

When choosing a Windows Client Platform delivery tool, System Center Configuration Manager and Microsoft Deployment Toolkit are options. See below for the feature comparison.

Capability	Microsoft Deployment Toolkit	System Center 2012 Configuration Manager (R2 SP1, SP2)	System Center Configuration Manager (Current Branch 1606)
Windows 10 Version Support	**1507, 1511, 1607**	**1507, 1511**	**1507, 1511, 1607**
Deploy UEFI/BIOS Platforms	X	X	X
Deploy applications during Task Sequence	X	X	X
Supports Image Creation	X	X	X
Lite Touch Deployment	X	X	X
Zero Touch Deployment		X	X
Manage a wide range of platforms		X	X
Increased Scalability (PXE, etc.)		X	X
Offline Image Servicing		X	X
Deploy Windows-to-Go		X	X
In-Place Upgrade		Task Sequence	Servicing

Edition

Overview

- Windows 10 supports business experiences using Windows 10 Professional and Enterprise editions
- Compare other Windows 10 editions online

	Professional	Enterprise
Windows Hello	✓	✓
Windows Defender	✓	✓
Windows Firewall	✓	✓
Virtual Desktops	✓	✓
Windows Information Protection	✓	✓
Azure AD Domain Join	✓	✓
BitLocker	✓	✓
Conditional Access	✓	✓
Windows Store for Business	✓	✓
Windows Update for Business	✓	✓
Current Branch for Business	✓	✓

	Professional	Enterprise
Enterprise State Roaming	✓	✓
Device Health Attestation	✓	✓
AppLocker	✓	✓
Direct Access	✘	✓
BranchCache	✘	✓
Windows to Go	✘	✓
Start & Taskbar Control	✘	✓
Credential Guard	✘	✓
Device Guard	✘	✓
App-V	✘	✓
UE-V	✘	✓
Long Term Servicing Branch	✘	✓

Strategy

Image Strategy	Thin Image	Hybrid Image	Thick Image
Windows Updates	X	X	X
Windows Features	X	X	X
Common Frameworks	X	X	X
LOB Applications		X	X
Common Productivity Apps		X	X
LOB used by Every Employee		X	X
Frequently Updated Frameworks			X
LOB Applications			X

Considerations

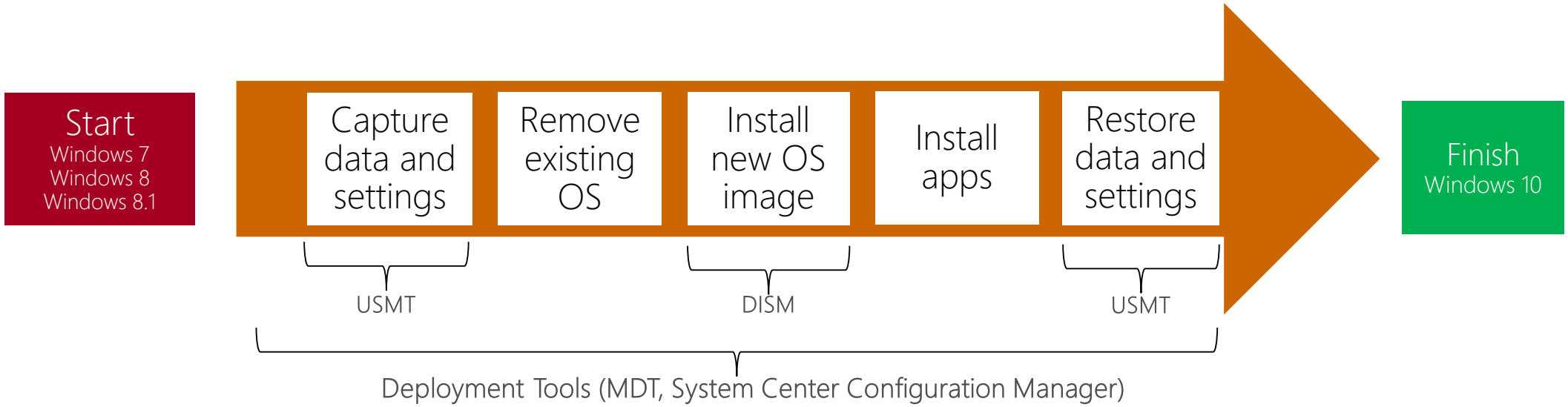
- Image revisions to support component and application updates
- Device deployment time
- Windows 10 1607 provides support for Sysprep via Windows as a Service, although image recreation is still the recommended approach

Wipe & Load Overview

Minimal changes to existing process

- Familiar with enterprises
- Out of the box support with Windows 7, Windows 8, and Windows 8.1
- Customized approach required to move from Windows XP/Vista to Windows 10
- Use System Center Configuration Manager or MDT for managing the process – requires update
- Administrator to configure preservation of existing apps, settings, and drivers

Wipe & Load (Refresh) Process



Deployment Methods

Deployment	Tools		Advantages	Scenarios
Offline Deployment	System Center Configuration Manager	Microsoft Deployment Toolkit	▪ No infrastructure required to deploy ▪ Support Challenges ▪ Challenging to maintain versioning	▪ Remote offices ▪ Limited network connectivity
Lite touch Deployment (LTI)			▪ Less engineering time than ZTI ▪ Requires interaction to initiate the deployment process ▪ Varied levels of automation supported	▪ Windows 10 Pilot ▪ Interactive deployment capability
Zero Touch Deployment (ZTI)			▪ Requires the most engineering time ▪ No user interaction required to initiate deployment ▪ 100% automation	▪ Organizations requiring high volume deployment capability

User State Migration

Overview	User state migration preserves user generated content, the user's customized experience of Windows, and application settings within the constraints of operating system and application compatibility
Supported Versions	Customers moving from earlier versions of Windows may choose to move to an intermediate Operating System version to allow full USMT support

	Windows Vista	Windows 7	Windows 8	Windows 8.1	Windows 10
Windows Vista	4.0	4.0, 5.0	5.0		
Windows 7		4.0, 5.0, 6.3	5.0, 6.3	6.3	Supported
Windows 8			5.0, 6.3	6.3	Supported
Windows 8.1				6.3	Supported
Windows 10				Supported	Supported

Platform Configuration

			Device Examples
Firmware	**BIOS**	▪ Flexible Deployment Media Support ▪ All legacy deployment methods still apply ▪ Maintain a single boot image	Devices purchased over 4 years ago
	UEFI (Recommended)	▪ Allows firmware to implement security policy ▪ Secure boot ▪ Faster boot times ▪ Latest UEFI Version required for compliance with Windows 10 Baseline and some features	Devices purchased within 4 years
Consideration		*Moving between UEFI and BIOS configurations is not supported through refresh scenario. The only supported way to move from UEFI to BIOS is through a **BARE METAL** (new device) deployment scenario, using PXE to boot into the device.*	

Driver Management

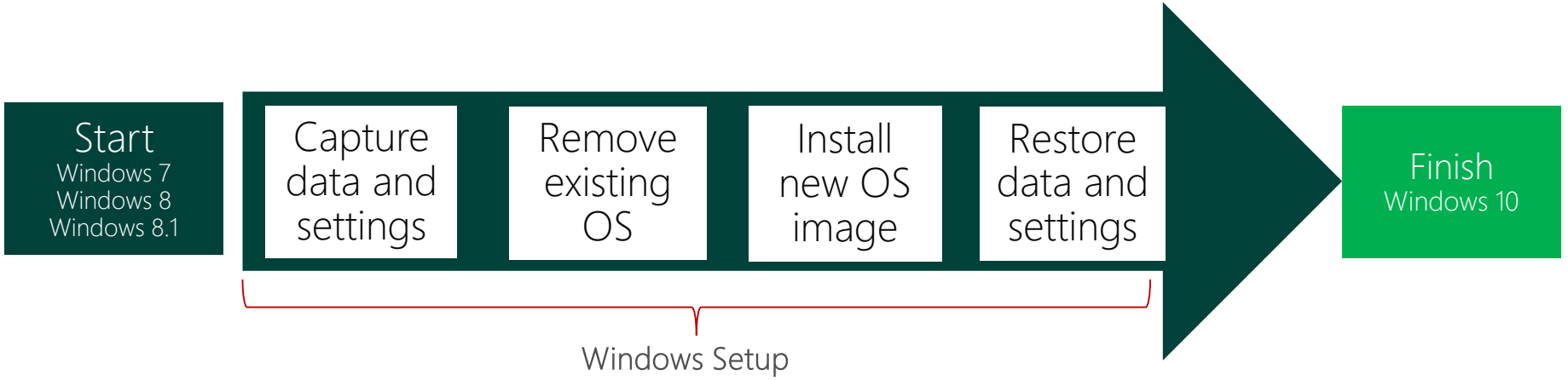
Option	Benefits	Limitations
Auto-Apply Drivers	▪ Easy to setup and maintain. ▪ Driver to client device matching 'just works'	▪ Less control over drivers chosen – first driver wins. ▪ If a problem occurs, troubleshooting is more difficult.
Apply Driver Packages (Recommended)	▪ Administrator can specify the exact driver for a particular make and model of client device. ▪ More control over each client device	▪ Additional up-front configuration and maintenance required.

Overview

Preferred Option for Enterprises

- Supported with Windows 7, Windows 8, and Windows 8.1
- Supported to upgrade Windows 10 1507 to 1511 and beyond
- Consumers use Windows Update, but enterprises want more control
- Use System Center Configuration Manager or MDT for managing the process
- Uses the standard Windows 10 image
- Automatically preserves existing apps, settings, and drivers
- Proven process - popular for Windows 8 to Windows 8.1 upgrade

In-Place Upgrade Process



Upgrade process -The Four Primary Phases

1 Down-level

Running Windows 7, 8, 8.1, 10

Check the system

Inventory Applications

Inventory Drivers

Assess compatibility

Prepare WinRE

2 Windows PE

Minimalist OS

Both new & old are offline

Backup down-level OS

Lay down new OS

Prepare new OS

- Inject drivers
- Some Migration

3 1st boot to new OS

Binding the new yoke

Specialize to the machine

Install drivers

Migrate Apps

More Migration

4 2nd boot to new OS

Finalize Upgrade

Welcome the user back

OOBE (skip if Win10 to another)

Ready **Set** **Go** **Welcome to Windows**

Upgrade vs Refresh

Why Upgrade?

- **Preserve applications, drivers, user data and settings -** Reduce upfront testing and deployment preparation
- **Compared to refresh, upgrade is…**
  - Faster – 30 to 60 minutes, on average, to upgrade
  - Smaller – file size is just the default OS media, no applications
  - More robust – "bulletproof" rollback on failure to functional down level system
- **Zero ADK dependencies**
- **Use it to supplement existing deployment scenarios -** Refresh, replace, and bare metal

Considerations

- **Compatibility with 3rd Party Disk Encryption tools** (BitLocker supported) – *Improved support for 3rd Party Disk Encryption with Windows 10 1607*
- **Upgrade process can be tested with pre-validation checks**
  - Trial run can be performed with Windows 10 Media using "/Compat ScanOnly" switch

Recovery

1 Down-level	2 Windows PE	3 1st boot to new OS	4 2nd boot to new OS
Clean-up	Boot to original OS Clean-up	Boot to recovery OS Reverse changes Cleanup Boot to Original OS	Boot to recovery OS Reverse changes Cleanup Boot to Original OS

5 Uninstall (limited time only)

Troubleshooting

Return Codes

- Minimum requirements not met to install the update (0xC1900200)
- System requirements not met for desired migration choice (0xC1900204)
- System does not pass the device scan to install the update (0x1900206)
- System does not pass the compat scan to install the update (0x1900208)
- System does not have enough free disk space (0xC190020E)

Log Check

C:\$WINDOWS.~BT\Sources\Panther

- Setup*.log – detailed logs
- *.xml – appraiser files with details about apps, drivers that aren’t compatible

Prepare for In-Place Upgrade

Perform a Pre-Validation Check

Use Windows 10 media to assess system readiness

Disk Encryption Compatibility

Check disk encryption technology support (if required)

Understand 3rd party ISV plans to support In-Place Upgrade approach

Work with Microsoft to address blockers

Plan Pilot Approach

Define success criteria

- Critical LoB and Web apps tested
- User Experience
- Group Policy / management configuration updates required

Plan for Content Distribution

Windows 10 Upgrade package size approximately 3.8Gb

Plan for content delivery to large, medium and branch sites

Utilize content caching technologies where required

Microsoft IT Camps – Windows 10 Cyber Defense & Security

AGENDA

- Begrüßung, Vorstellung, Erwartungen
- Einführung Windows 10
- Neuer Ansatz Mobility
- Windows 10 Servicing
- Windows 10 Deployment
- Windows 10 Provisioning
- Weitere Tools

Welche Bereitstellungsoptionen gibt es?

Old-school-Methode	In-Place	Provisioning Packages
• Daten und Einstellungen sammeln • **Golden** Image • Treiber werden eingespielt • Apps werden eingespielt • Daten und Einstellungen wiederherstellen	• Daten, Einstellungen und Treiber bleiben erhalten • minimalistisches Betriebssystem	• Bring Your Own Device Szenario • Daten, Einstellungen und Treiber können hinzugefügt werden • Edition Upgrades können durchgeführt werden • Sicherheitseinstellungen können gesetzt werden

Welche Bereitstellungsoptionen gibt es?

Wipe and Load	In-Place	Provisioning Packages
• "bare metal" - neue Hardware • "refresh" - neues OS • "replace" - Upgrade	• Manuell durch Benutzer • Windows Update durch Benutzer • WSUS durch Benutzer/Admin • Teil-/ Vollautomatisiertes durch Benutzer / Admin	• Standalone ausgeführt • Innerhalb einer Task-Sequenz

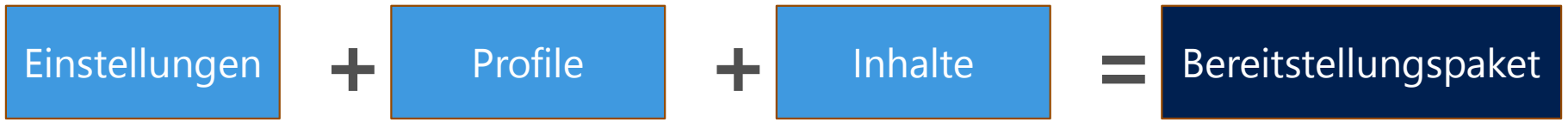
Provisioning Packages

Was ist ein Bereitstellungspaket im Detail?

Format der Bereitstellungspakete ist *.PPKG (WIM Container)

Inhalt von Bereitstellungspaketen:

- Einstellungen
- Profile
- Inhalt (Daten, Setups, …)



Provisioning Packages

Editionsupgrades
- Angabe des Lizenzschlüssels für ein Editionsupgrade

Initiales Setup
- Computername (Prefix + Zufallszahl oder Seriennummer)
- Anlegen von lokalen Benutzern, Passworten und Gruppen

Integration in Unternehmen
- Beitritt in ein lokales Active Directory
- Beitritt in ein Azure Active Directory
- MDM Enrollment

Provisioning Packages

Windows Apps
- Installation von Store Apps
- Deinstallation bereits vorhandener Apps

Win32 Scripts
- Ausführung von Scripts (PowerShell) und Installation von MSI Paketen

Konnektivitätsprofile
- WLAN
- Proxyeinstellung
- E-Mail

Provisioning Packages

Unternehmensrichtlinien/Sicherheitseinschränkungen
- Kennwort
- Verschlüsselung

Zertifikate
- Stammzertifizierungsstelle (CA)

Anpassung des Startmenüs
- Layout des Startmenüs
- Anheften von Anwendungen

Windows 10 Enterprise Serie - Windows Provisioning MICROSOFT

Guido Arenz | 26.02.2016 | 2
Tags: Windows 10, Provisioning

>> zur Übersicht und Einleitung der Blogserie "Windows Enterprise Serie"

Mit Windows 10 können Bereitstellungspakete erstellt werden, die das schnelle und effiziente Konfigurieren eines Geräts ermöglichen ohne ein neues OS Image installieren zu müssen. Bereitstellungspakete sind so einfach aufgebaut, dass Benutzer ohne technischen Hintergrund nur eine kurze schriftliche Anleitung benötigen, um damit ihr Gerät zu konfigurieren. Dies kann eine erhebliche Einsparung in Bezug auf den Zeitaufwand bedeuten, der zum Konfigurieren einer größeren Zahl von Geräten in einem Unternehmen anfällt.

Provisioning Packages

Vorteile:

Schnelles Konfigurieren eines neuen Geräts ohne Installation eines neuen Images

Konfiguration von mobilen Geräten und Desktops bzw. Notebooks mit Bereitstellungspaketen

Schnelles Konfigurieren der eigenen Geräte von Mitarbeitern in einer Organisation ohne Infrastruktur für die mobile Geräteverwaltung (MDM)

Einrichten eines Geräts, ohne dass für das Gerät eine aktive Netzwerkverbindung erforderlich ist

Wrap Up Provisioning Packages

Mit Bereitstellungspaketen können Sie…	Für Bereitstellungspakete…
Endbenutzern über USB, FTP, E-Mail ein Konfigurationspaket zukommen lassen	benötigen Sie lokale Administratorenrechte
zur Laufzeit Geräte von Endbenutzern (Notebooks, Desktops, Smartphones) konfigurieren	benötigen Sie manuelle Interaktion (keine Kommandozeile). Eine „Installation“ über eine SW-Management Lösung ist nicht möglich.
mit Hilfe von DISM, Konfigurationen innerhalb ihres Images aufnehmen	gibt es kein „wirkliches“ Rollback
	wird Crapware / Bloatware nicht immer berücksichtigt

Microsoft IT Camps – Windows 10 Cyber Defense & Security

AGENDA

- Begrüßung, Vorstellung, Erwartungen
- Einführung Windows 10
- Neuer Ansatz Mobility
- Windows 10 Servicing
- Windows 10 Deployment
- Windows 10 Provisioning
- Weitere Tools

Device Protection

Microsoft Bitlocker Administration & Monitoring

Capability	BitLocker + Active Directory Environment	MBAM + BitLocker Environment
Key Escrow	X	X
Key Recovery	X	X
Policy Application	X	X
Advanced Compliance Reporting		X
Key Recovery Auditing		X
TPM Enablement/Deployment		X
Self Service Key Recovery		X

Data Separation & Leak Protection

Windows Information Protection

Overview	▪ Provides integrated protection against accidental data leaks
Features	▪ Protects data at rest locally and on removable storage ▪ Corporate vs personal data identifiable wherever it rests on the device and can be wiped ▪ Prevents unauthorized apps from accessing business data and users from leaking data via copy and paste protection ▪ Common experience across all Windows 10 devices with copy and paste protection
Pre-Requisites	▪ Windows 10 1607 ▪ Microsoft Intune or System Center Configuration Manager (1606 or later)
Implementation	▪ Policy configured by System Center Configuration Manager or Microsoft Intune ▪ Device receives policy and is configured for Windows Information Protection

Data Separation & Leak Protection

Windows Information Protection

How it works

- Relies on existing OS encryption technology - EFS used for Work Folders in Windows 8.1
- Supports both Modern and Win32 applications
- Better together with Azure Rights Management for:
  - Saving enterprise data to USB drives
  - Sharing enterprise data via email
  - Synchronizing data to public cloud storage or other services

Define Enterprise Boundaries

Enterprise boundaries are defined in one of two ways:

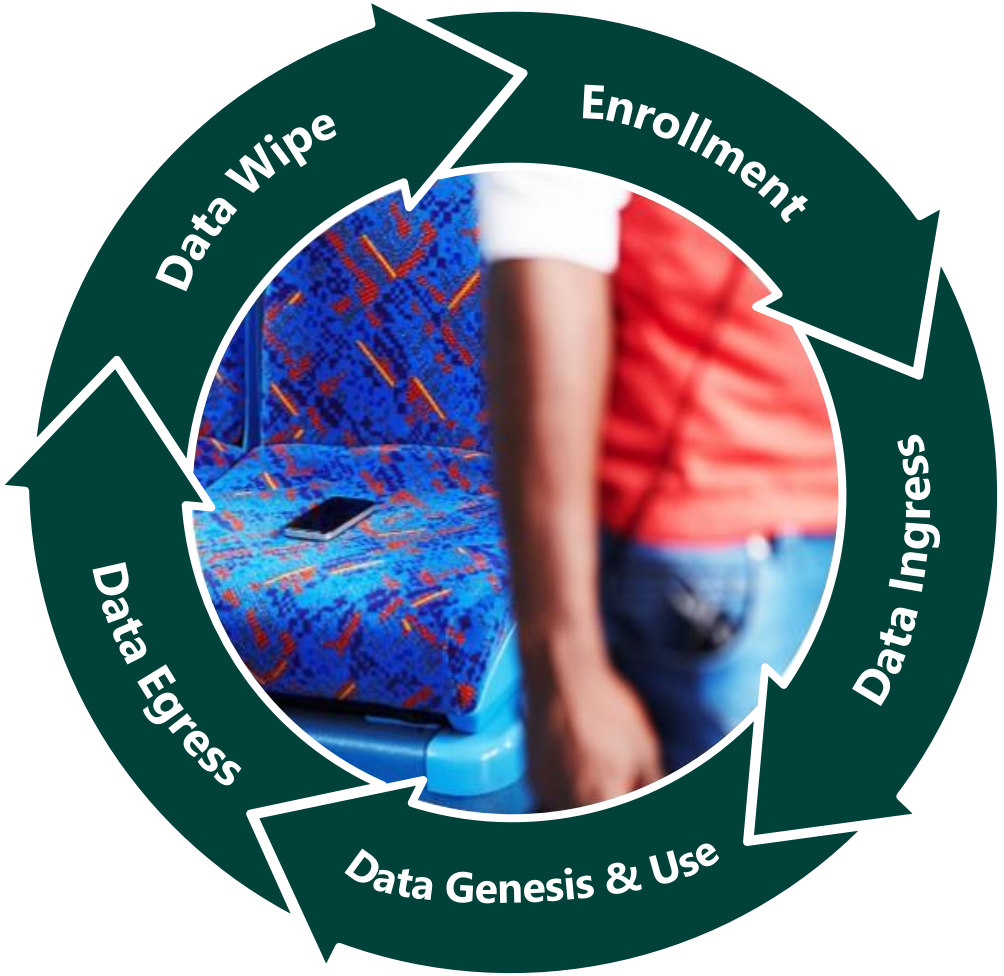
- Administrator defines a set of enterprise approved applications that are allowed to access data
- Network Boundaries are defined (IP ranges, Cloud locations e.g. O365) - Defines if data is coming from or going to a defined "Enterprise" location

Configure Windows Information Protection

Administrators can configure Windows Information Protection in one of three ways:

- Blocking
- Policy Override
- Reporting Only

Windows Information Protection Lifecycle



Policy provisioned to device

Data coming from corporate network location automatically protected by WIP

App can automatically protect data or users can define data as personal or corporate

Protection can be maintained anywhere on the device or when data moves to removable storage. RMS can be used to maintain protection in B2B scenarios.

Selectively wipe corporate data demand or when device is unenrolled

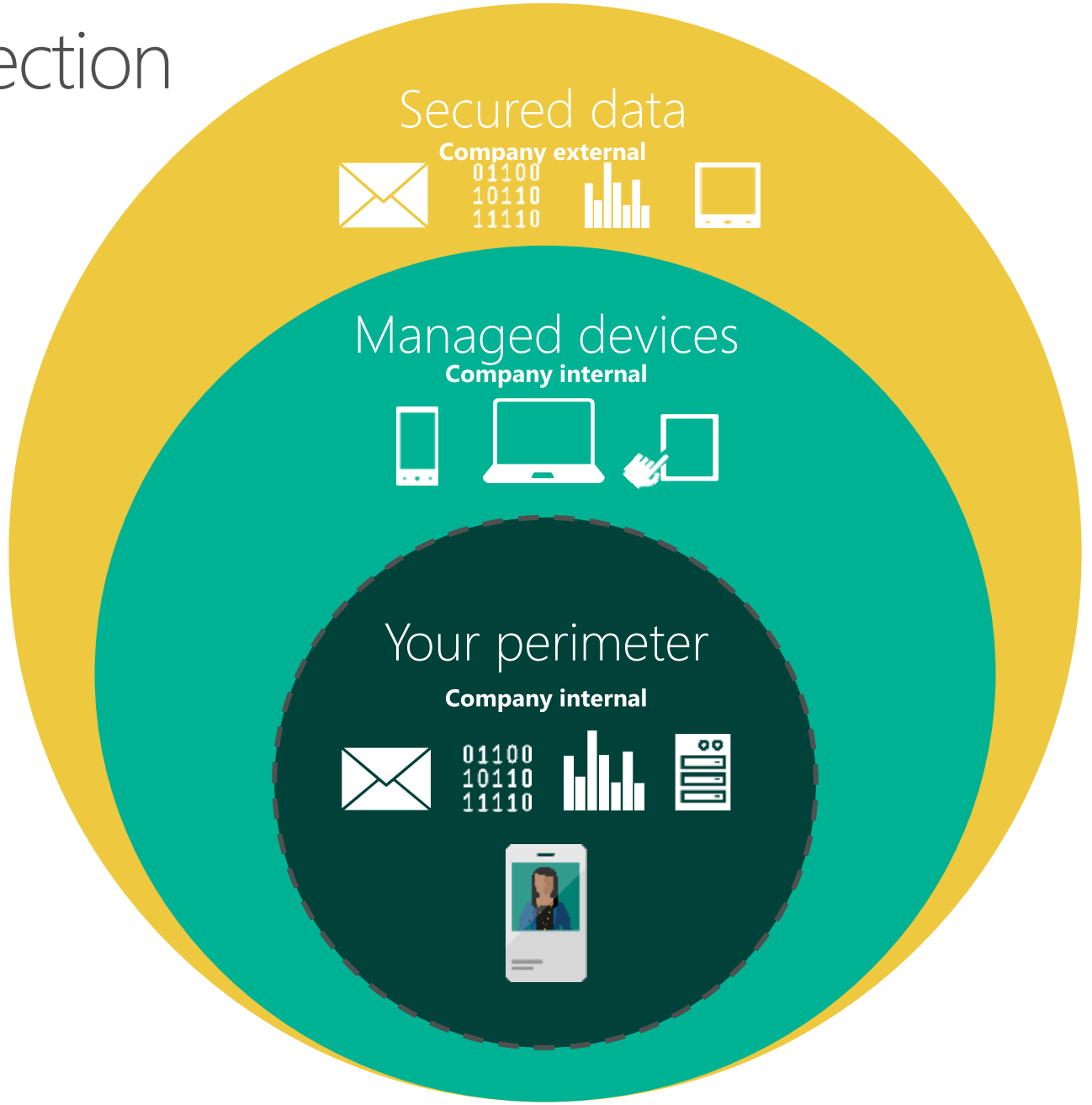
Data Leak & Data Sharing Protection

Challenges

You have a perimeter

You have managed devices within a broader perimeter

Your business requires you to store and/or share sensitive data outside of your on-premises boundary



Data Leak & Data Sharing Protection

How to solve?

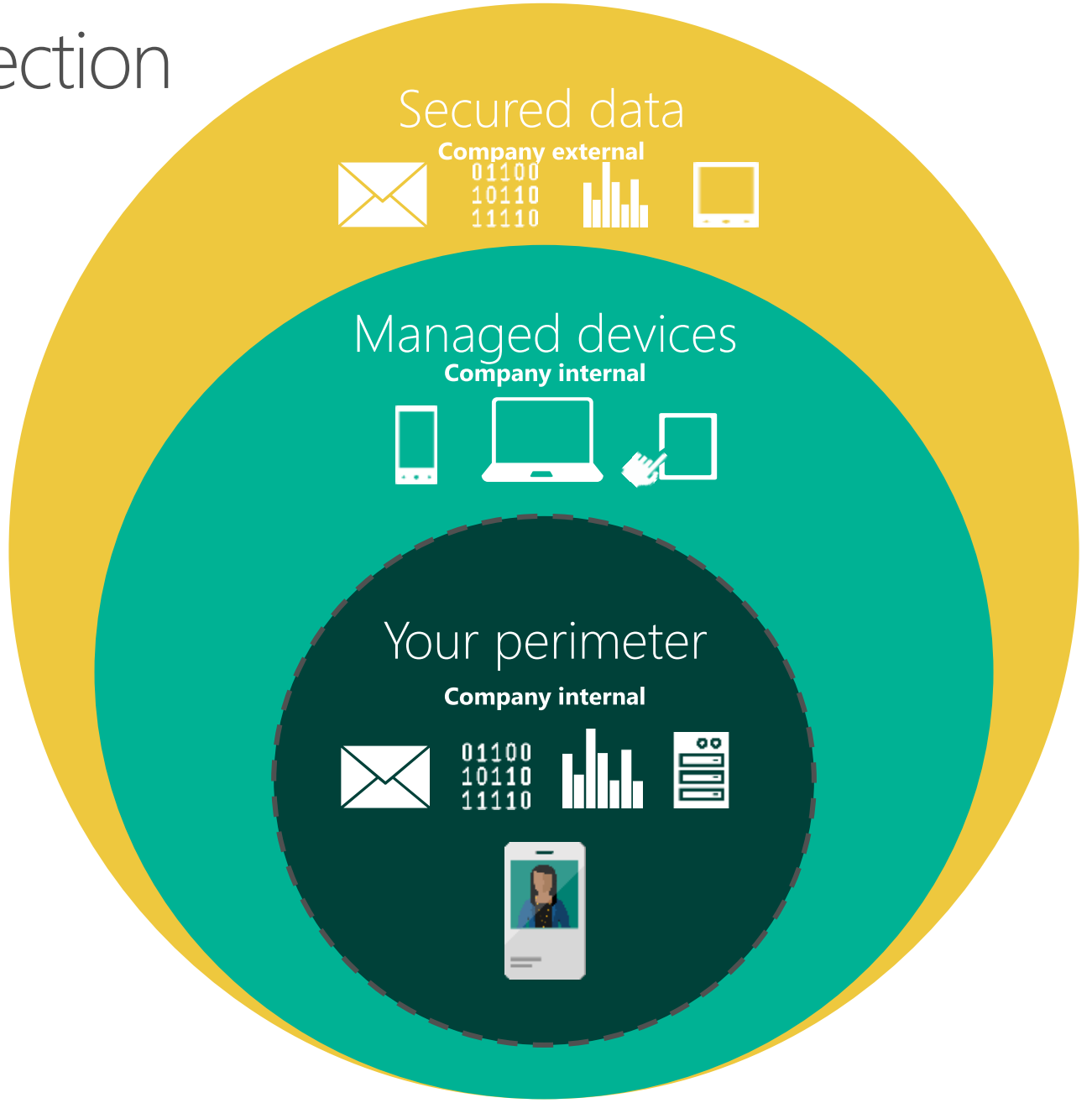
Keep all data on premises?!?

Managing all identities
in your own directory?!?

Lock down devices, PCs, and
users to restrictive policy?!?

Accept that data will leak?!?

Or ....

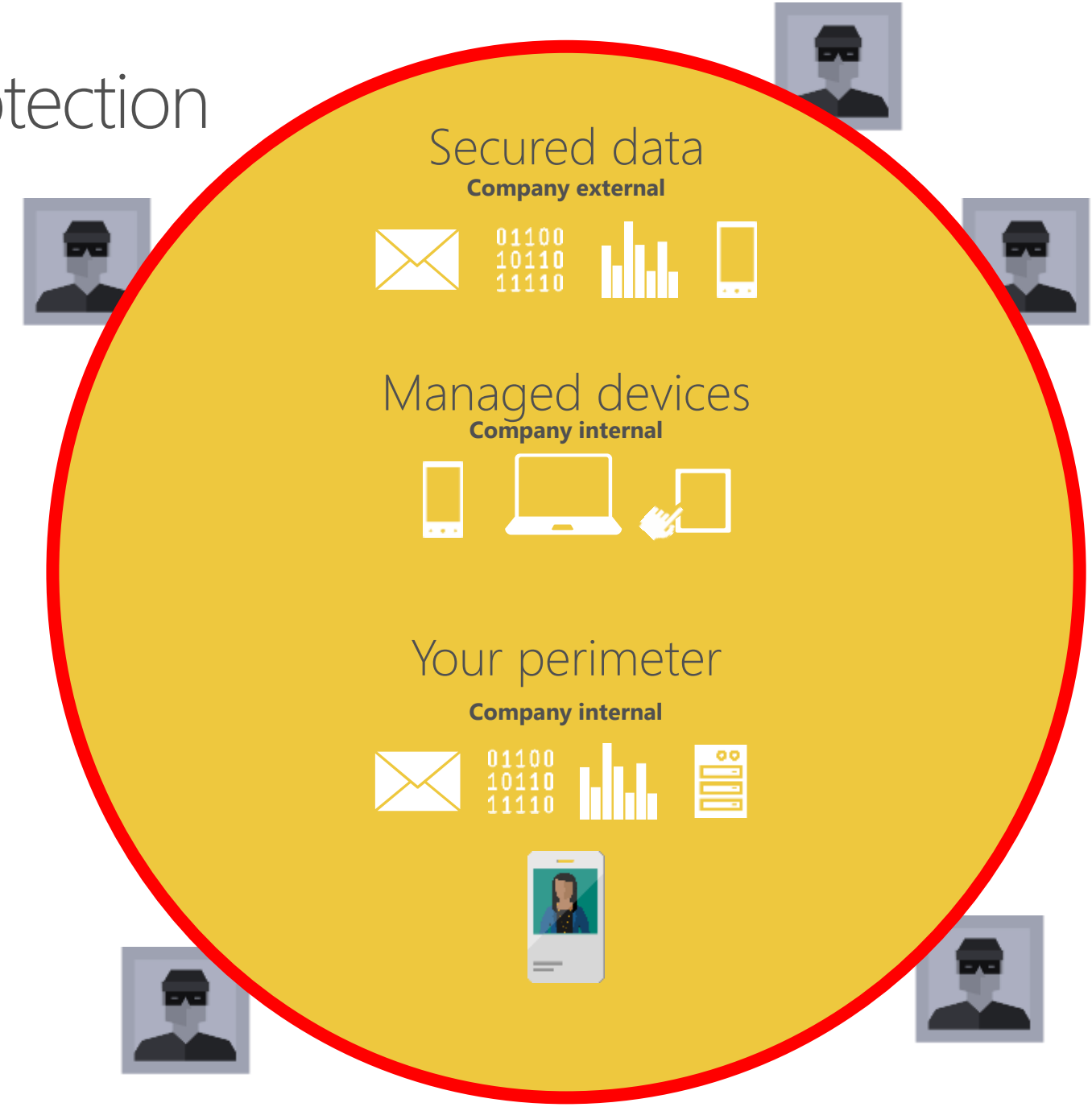


Data Leak & Data Sharing Protection

Identity Bound Protection

Disparate storage requires the data itself to be protected.

External sharing of data requires identity-bound data protection



Data Leak & Data Sharing Protection

Azure Information Protection

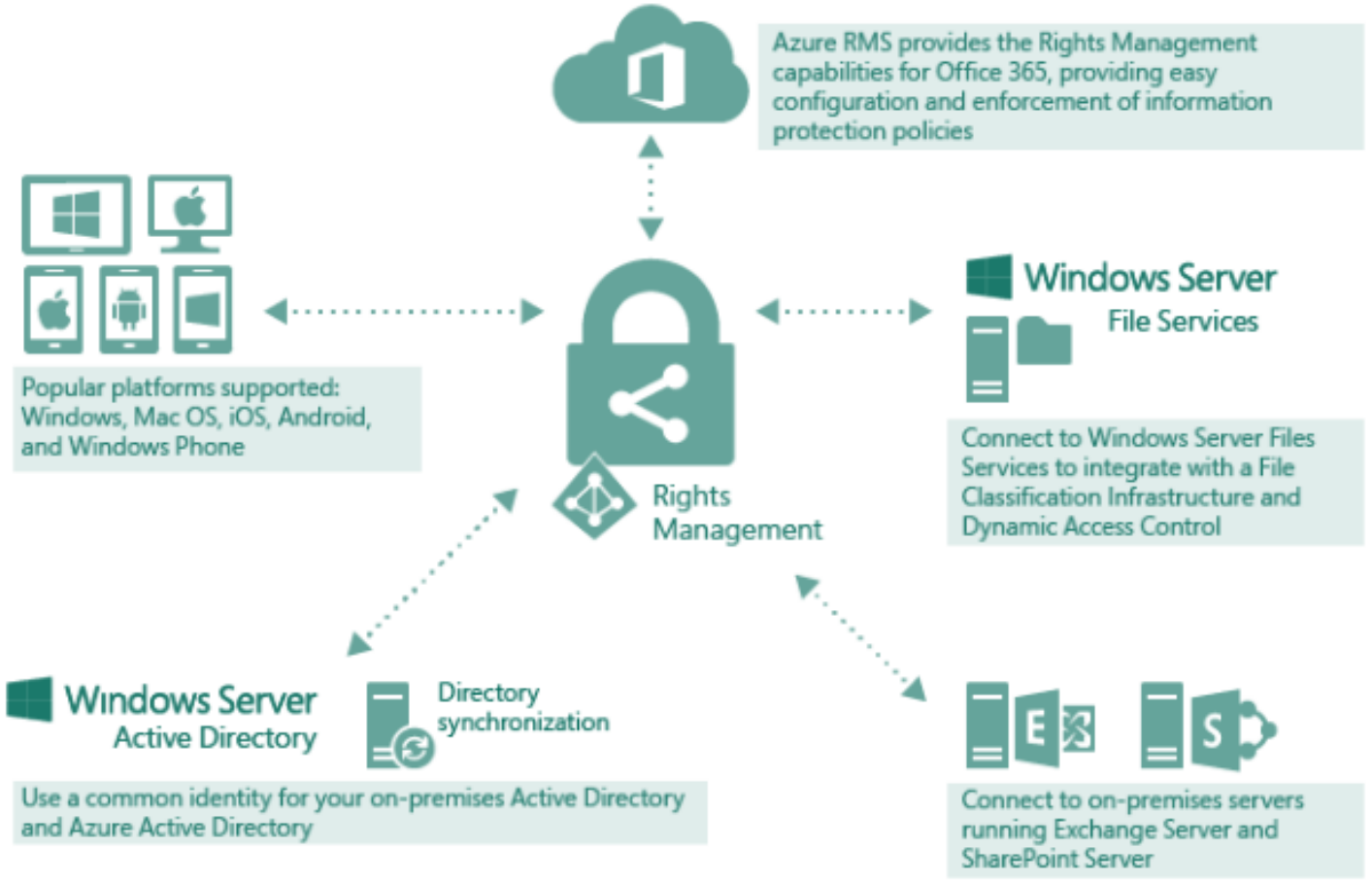
Overview	▪ Combination of Microsoft Azure Rights Management & acquisition of Secure Islands data classification technology ▪ Identity driven approach to security ▪ Available in Public Preview
Features	▪ Classify, label and protect data at the time of creation or modification ▪ Persistent protection that travels with your data ▪ Enable safe sharing with customers and partners ▪ Simple, intuitive controls help users make the right decisions and stay productive ▪ Visibility and control over shared data ▪ Deployment and management flexibility
Requirements	▪ Azure Subscription that includes Azure Rights Management Services ▪ Global Administrator rights to activate the Rights Management service ▪ Windows 7 SP1 device or above, with Office 2010 and above

Data Leak & Data Sharing Protection

Azure Rights Management Services

Capabilities

- Protect all file types
- Protect files anywhere
- Share files securely by email
- Auditing and monitoring
- Support for commonly used devices
- B2B collaboration
- Support for Office 365 and on-premises services



Vielen Dank


Windows 10