

Herzlich Willkommen
zum Microsoft IT Camp
Windows 10 Enterprise Deployment



Eric Berg



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/>



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®



Microsoft IT Camps – Windows 10 Enterprise Deployment

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 Enterprise Deployment

AGENDA

- Begrüßung, Vorstellung, Erwartungen

- Einführung Windows 10
- Neuer Ansatz Mobility
- Windows 10 Servicing
- Windows 10 Deployment
- Windows 10 Provisioning
- Weitere Tools





Du bist hier: [IT-Camps](#)

IT-CAMPS: AGENDA SLIDES SPEAKERPROFILE ▾ LINKS & DOWNLOADS



IT-Camps

Herzlich Willkommen zu den IT-Camps!

Wir freuen uns, dass du dabei bist!

In diesem ganztägigen Workshop fokussieren wir die wichtigsten Neuerungen, Features und Produkte innerhalb und rund um Windows 10. Das bearbeiten wir die beiden Schwerpunkte:

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

in jeweils eigenen Tagesveranstaltungen.

Alle Infos zu den Inhalten beider Camps, Verlinkungen, Downloads etc. findest du auf dieser Seite. Solltest du dich für weitere IT-Camps 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.



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 Enterprise Deployment

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

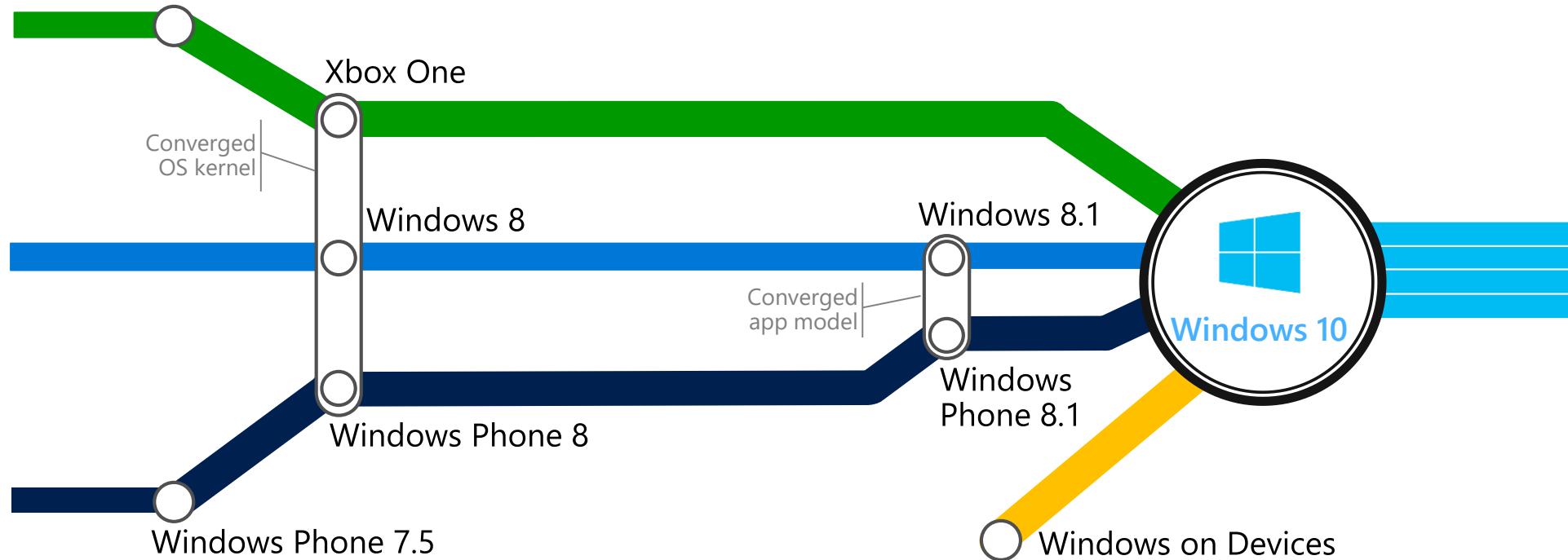
2015

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 Enterprise Deployment

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

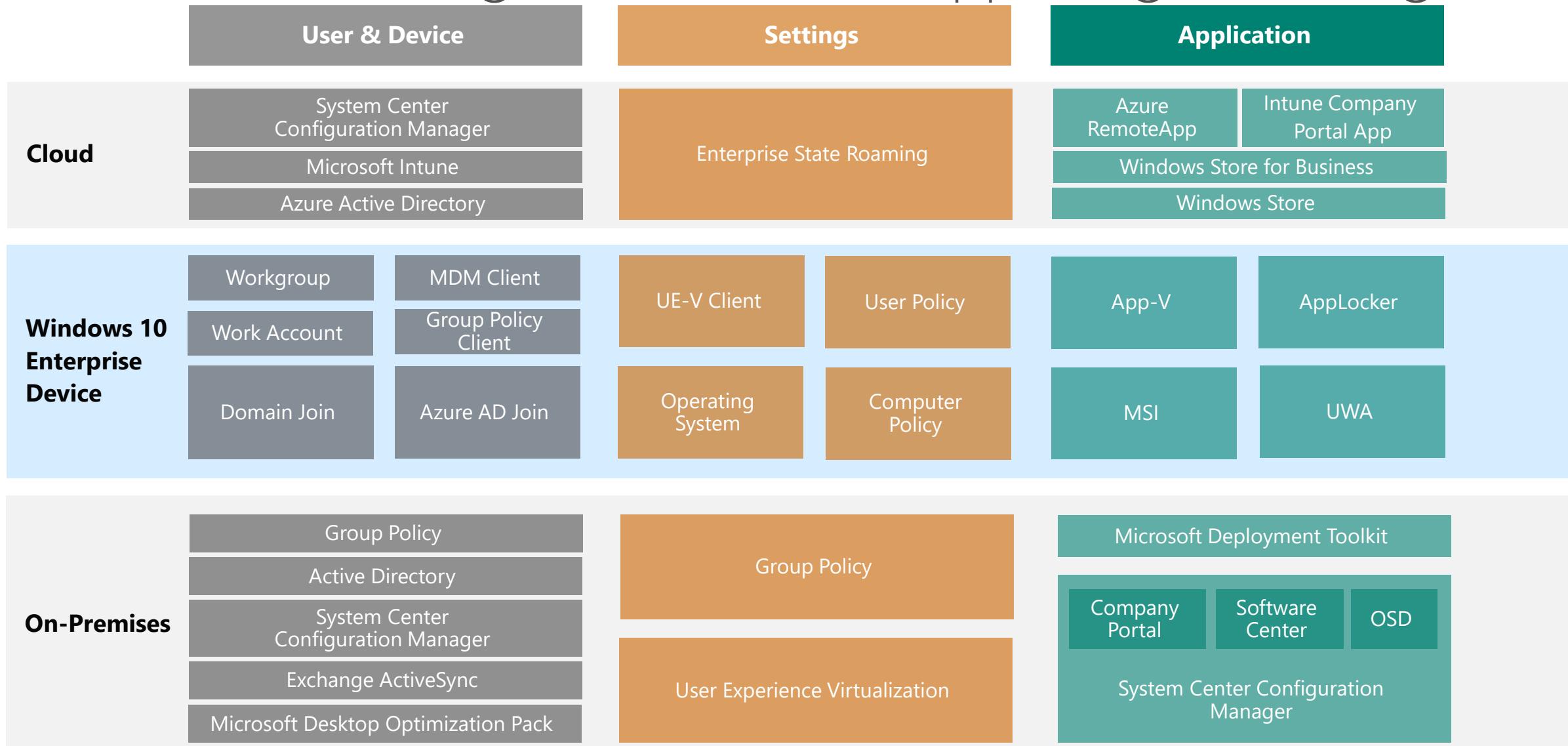
Ownership

- Corporate Owned
- Choose Your Own Device
- Bring Your Own Device

Management Capability & Scenario Matrix

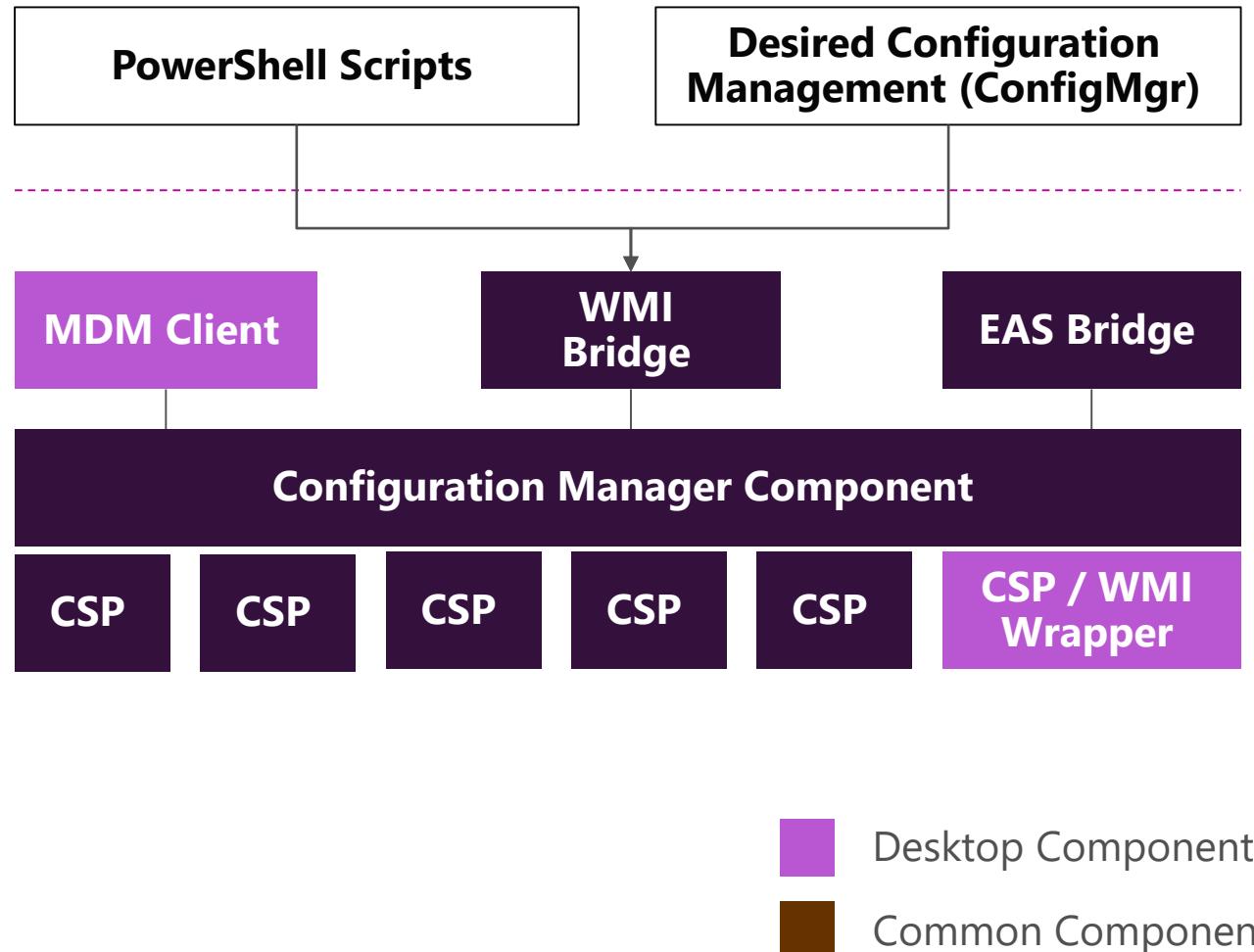
	Capabilities	Scenarios			
		Evergreen Windows 10 management	Take control of mobile devices	Familiar user experience	Reduce device onboarding costs
User & Device	Traditional Management	✓	✗	✓	✗
	Modern Management	✓	✓	✓	✗
	Provisioning	✗	✗	✗	✓
Settings	Policy Configuration	✓	✓	✓	✓
	OS Customization	✗	✓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

Windows 10 Management Stack & Supporting Technologies



Management Architecture

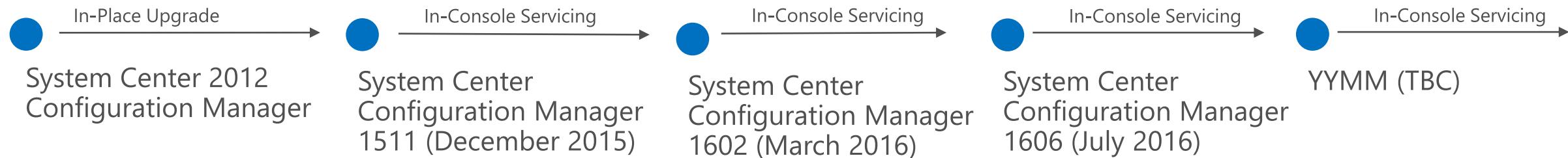
- Alternative method to Group Policy management.
 - Companies may use both approaches to manage devices .
-
- MDM client on Windows 10 talks through Configuration Manager component (not System Center) to other components including Configuration Service Providers (CSP) for additional MDM features / functionality
-
- WMI Bridge exposes MDM settings available, which administrators can be configured via DCM (ConfigMgr) or PowerShell



System Center Configuration Manager

Lifecycle

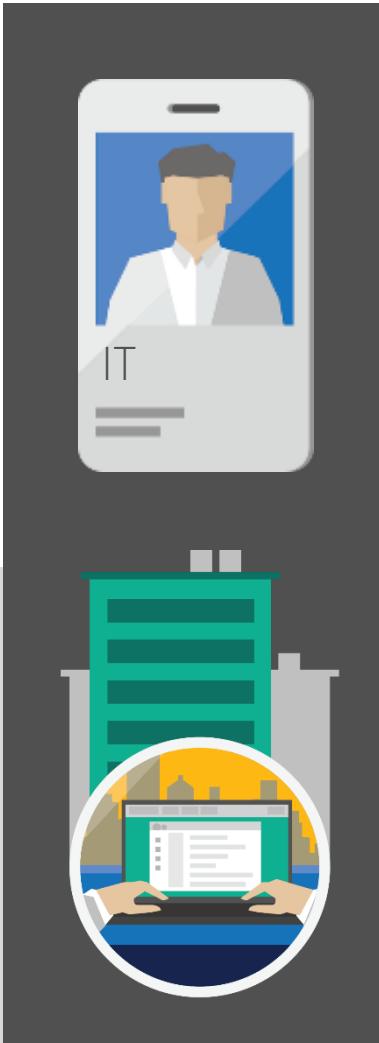
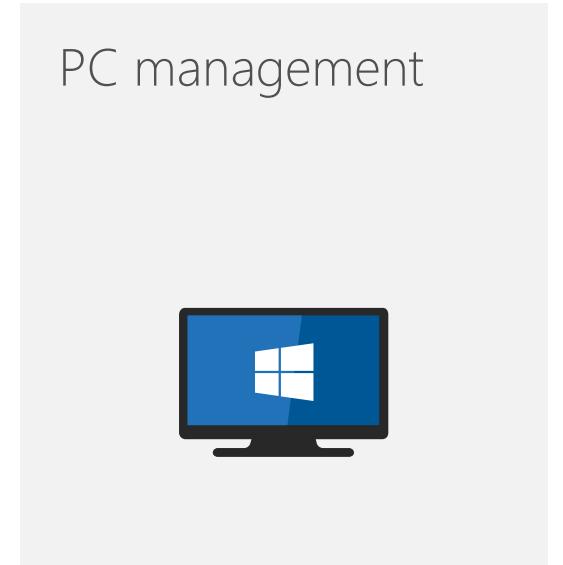
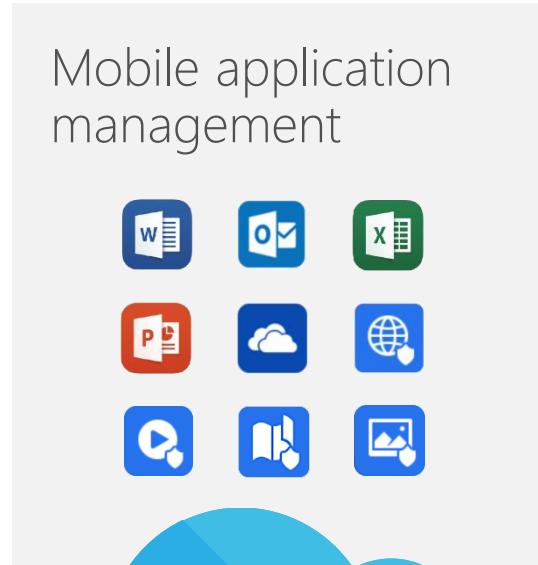
Product version	Release vehicle	Availability	Features supported	Support	Windows Servicing Model supported
System Center Configuration Manager	Current Branch	December 2015 with updates released periodically throughout the year	New features, security updates, bug fixes	Can defer updates for up to 12 months 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

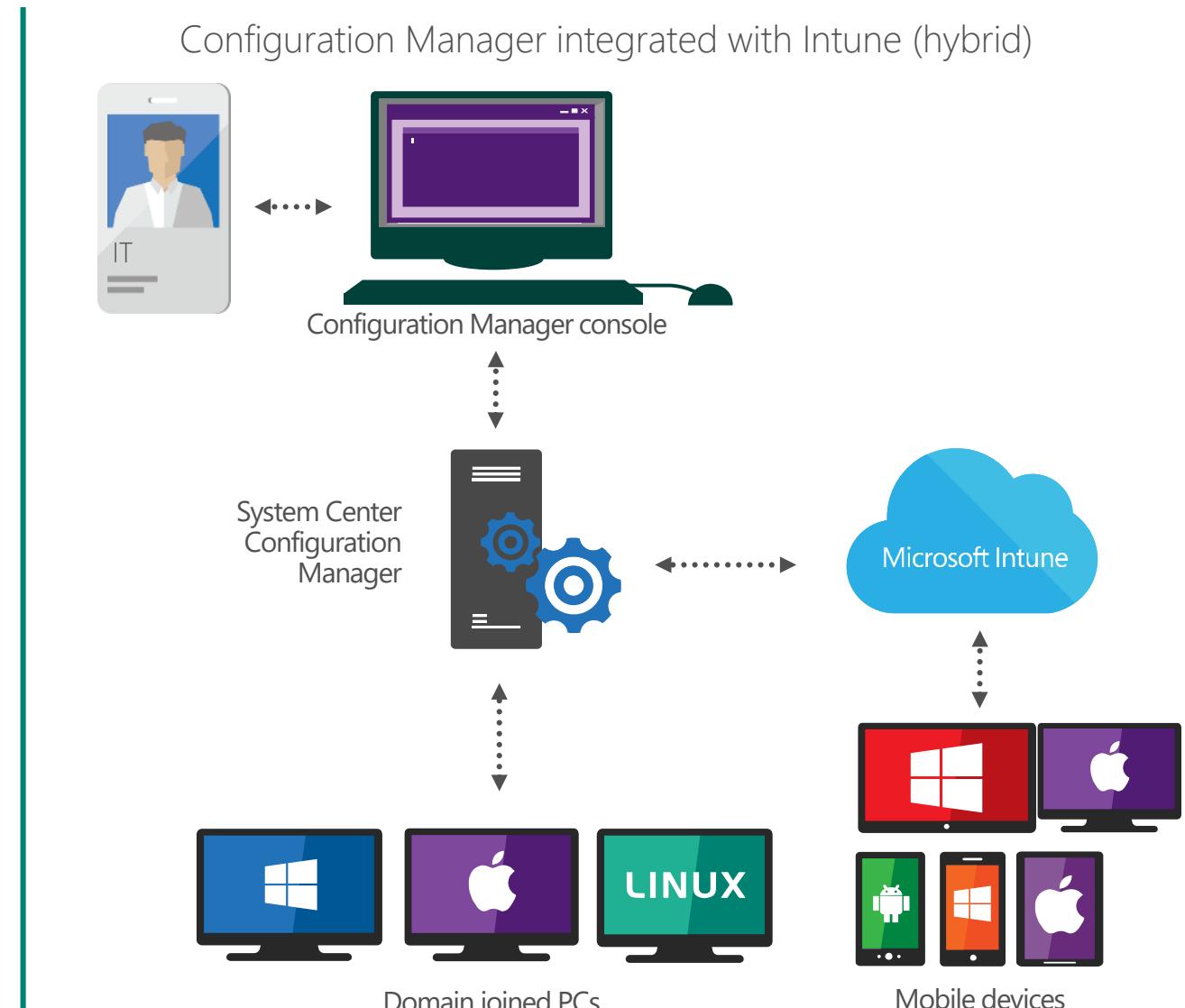
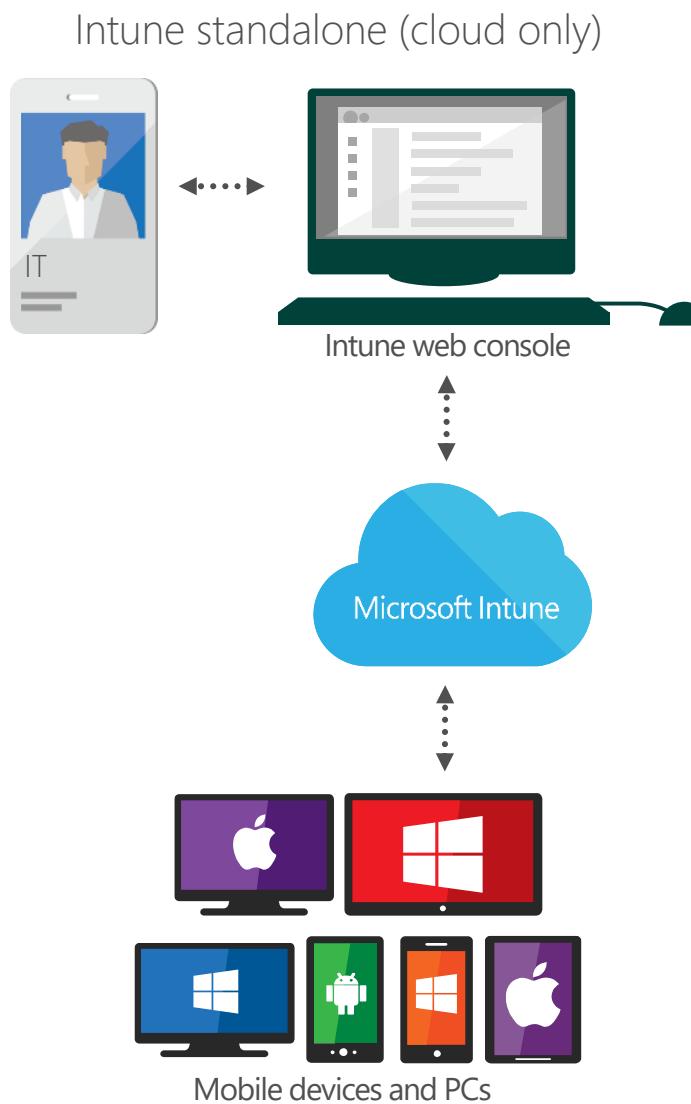
System Center Configuration Manager Version	Windows 10 Version			
	LTSB 2015	1507	1511	1607
2007	Management Only			
2012 SP2 or R2 SP1				
1511				
1602				App Compat of Current Branch
1606				

Modern Management with Microsoft Intune



Intune helps organizations provide their employees with access to corporate applications, data, and resources from virtually anywhere on almost any device, while helping to keep corporate information secure.

Microsoft Intune Deployment Flexibility



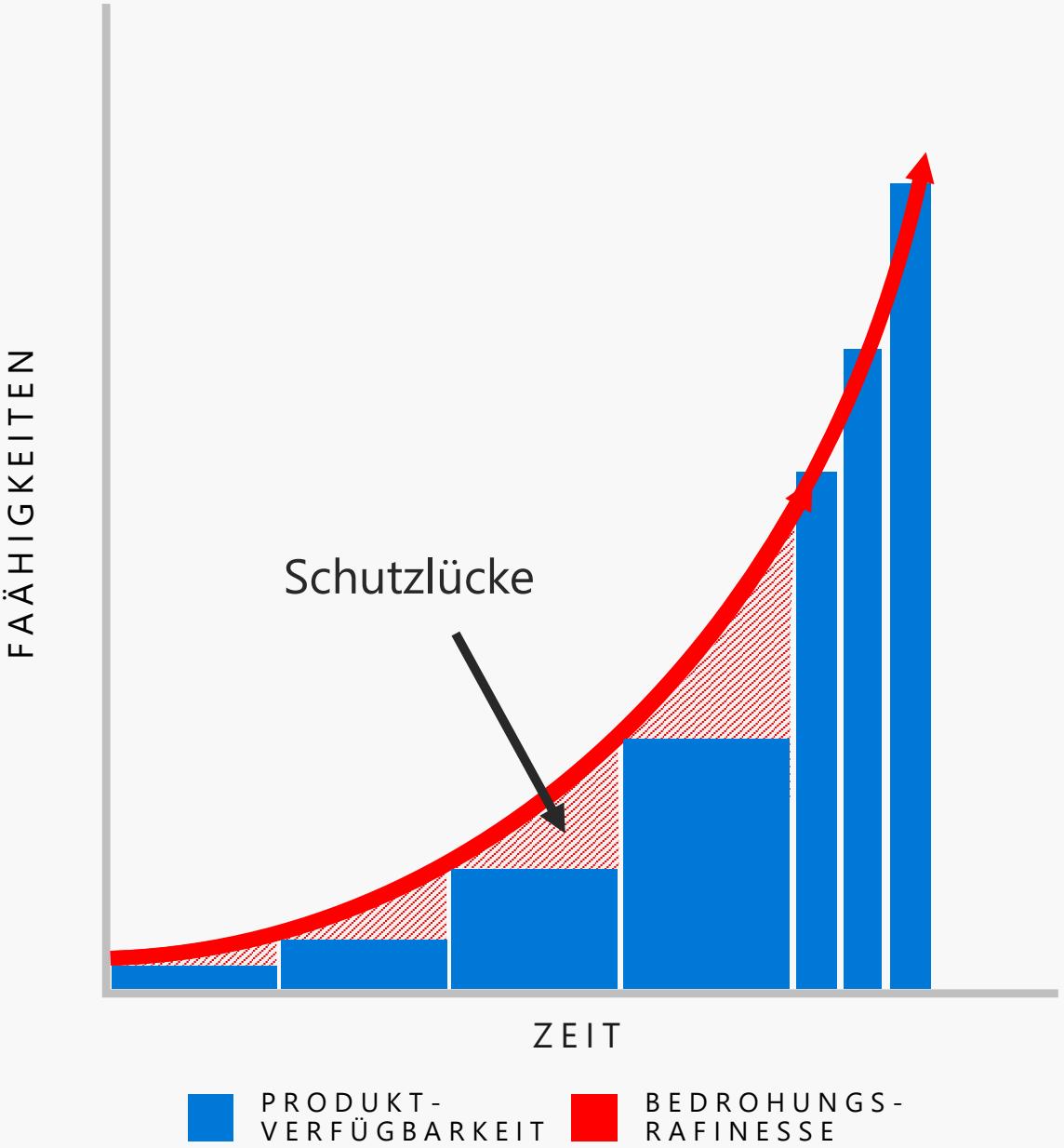
Microsoft IT Camps – Windows 10 Enterprise Deployment

AGENDA

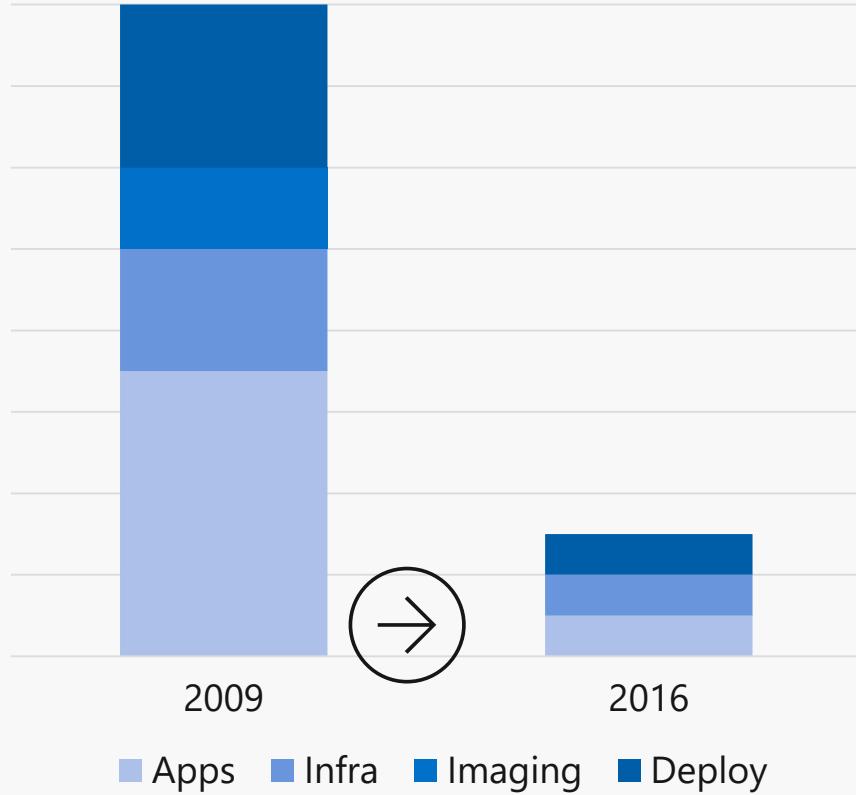
- Begrüßung, Vorstellung, Erwartungen
- Einführung Windows 10
- Neuer Ansatz Mobility
- Windows 10 Servicing
 - Windows 10 Deployment
 - Windows 10 Provisioning
 - Weitere Tools

Bedrohungsabschitz Während Zeit Software as a Services

Angriffszenarien über Zeit
durchgängig Reaktion
zerstört



Simplifying Deployment with Windows 10



No more big deployment projects

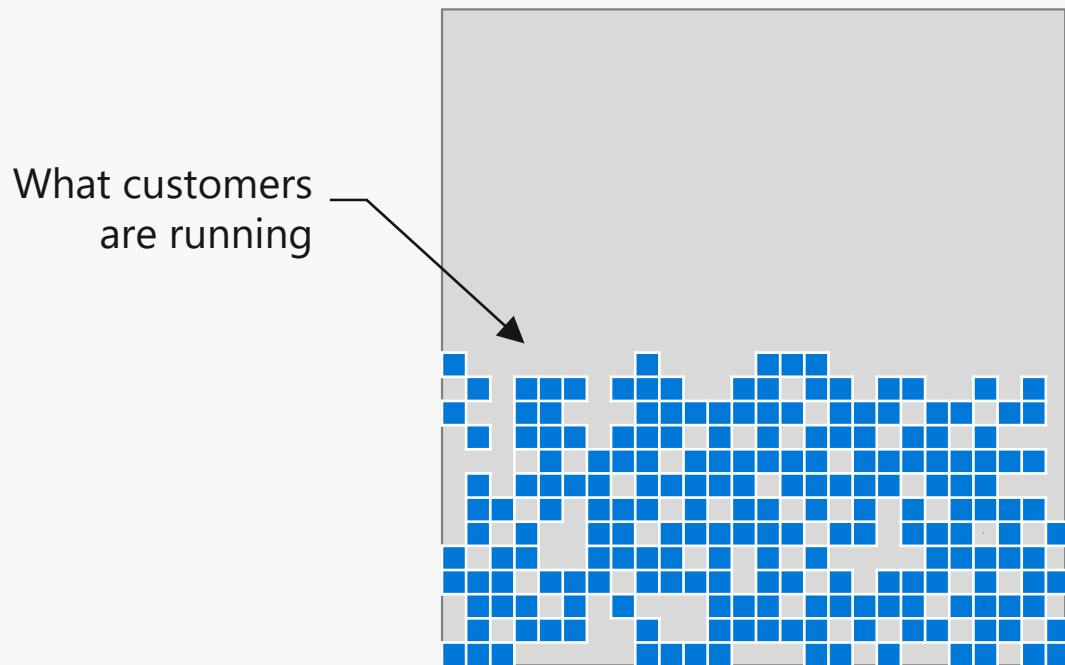
Incremental changes, delivered more frequently

Easy, automated deployment processes

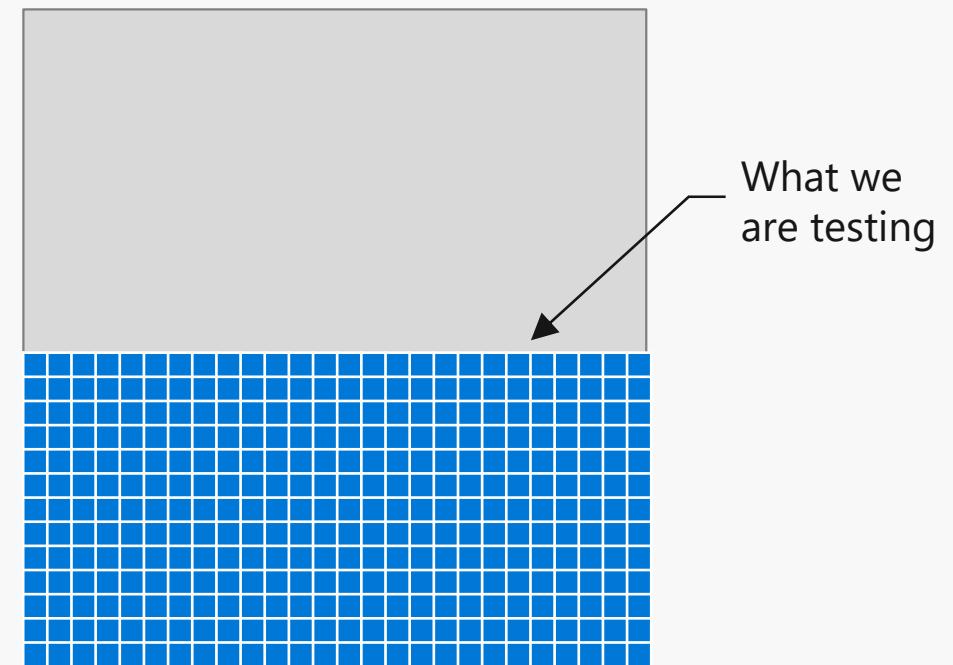
Exceptional application compatibility

Windows as a service: Servicing Windows

With Windows 7 and 8, servicing choices added complexity and cost, increased fragmentation, and reduced quality



Typical Windows 7 PC:
Selectively Patched



Windows 7 Test Lab PC:
Fully Patched

Introducing Windows as a Service

A brand new way of building, deploying, and servicing Windows

Building

Continual, ongoing development

Deliver new features twice per year

In the open, to enable and encourage feedback



Deploying

Stay current with simple, automated update process

Unmatched application compatibility

Flexible timelines, methods, tools



Servicing

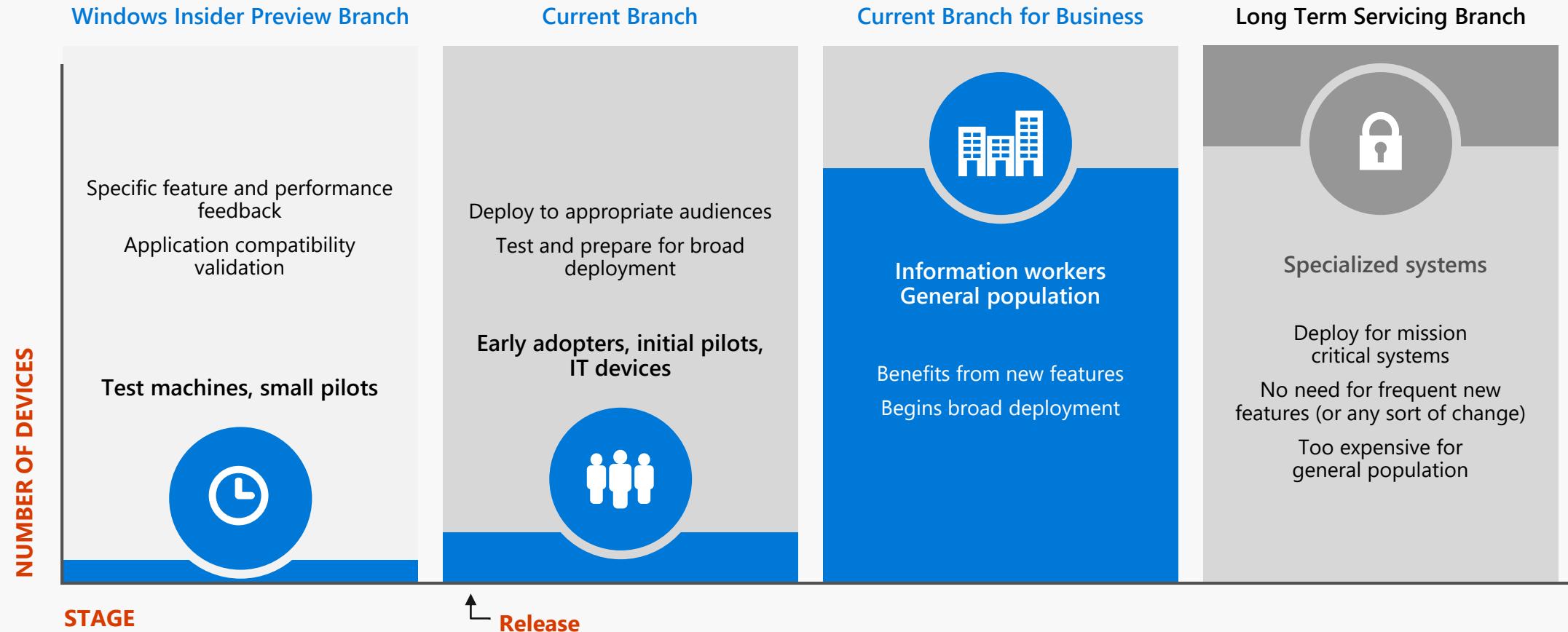
Simplified process, to ensure consistency, stability and reliability

Delivered using cumulative updates

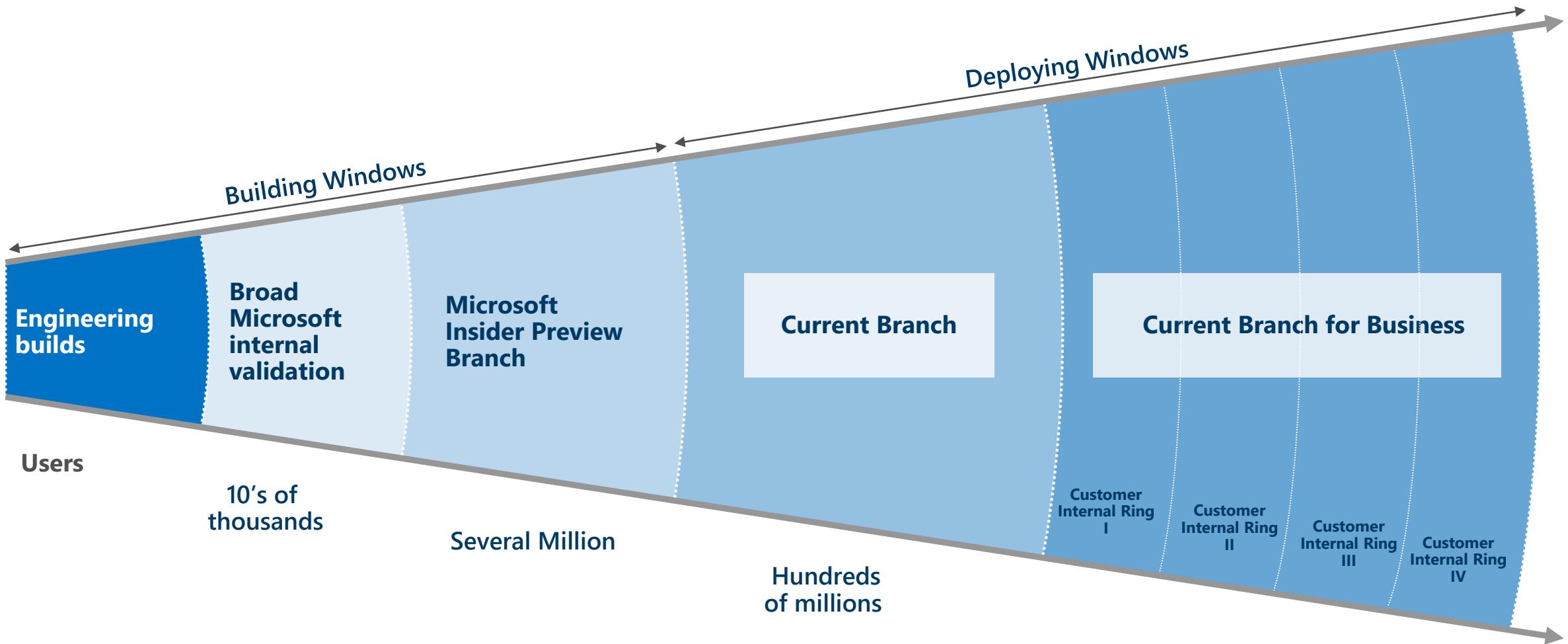
Eliminate platform fragmentation for all Windows-based devices

Windows as a service: Deploying Windows

Unmatched flexibility and control, depending on needs

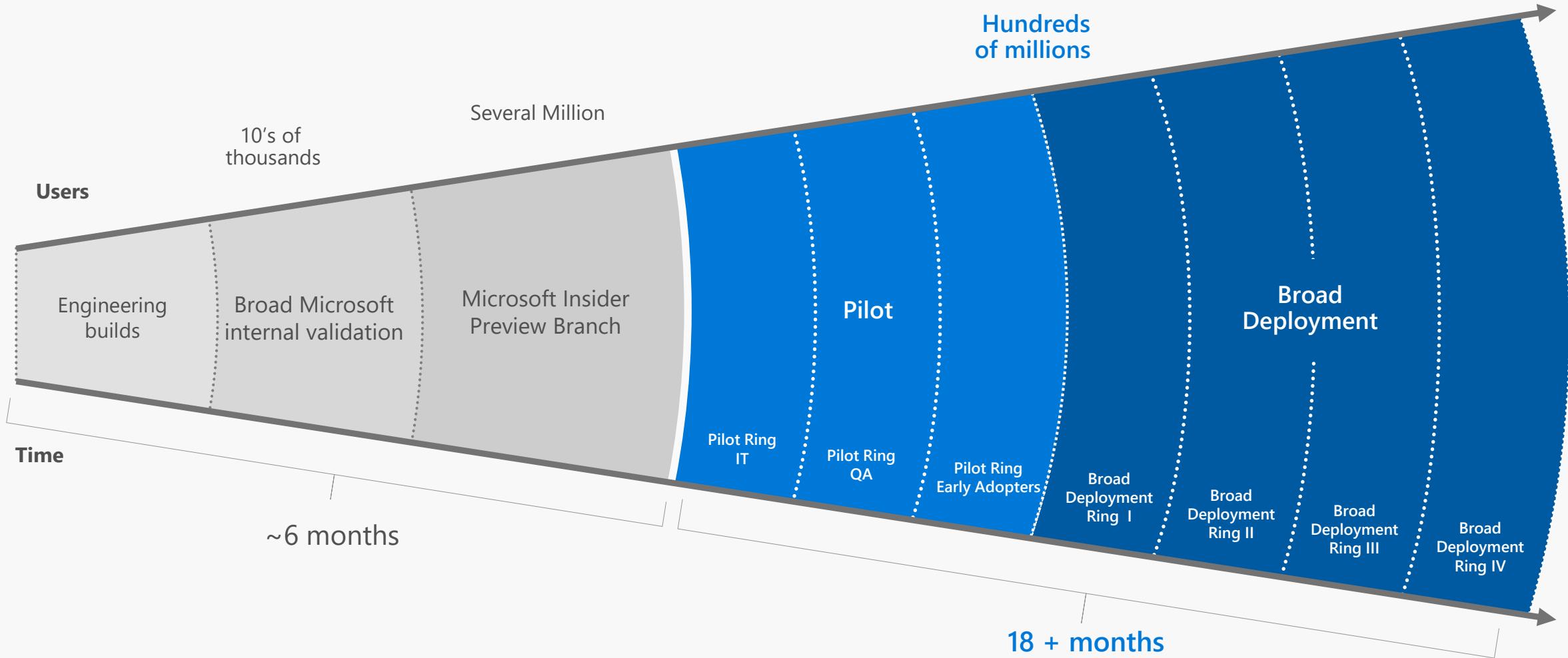


Windows as a Service Branches



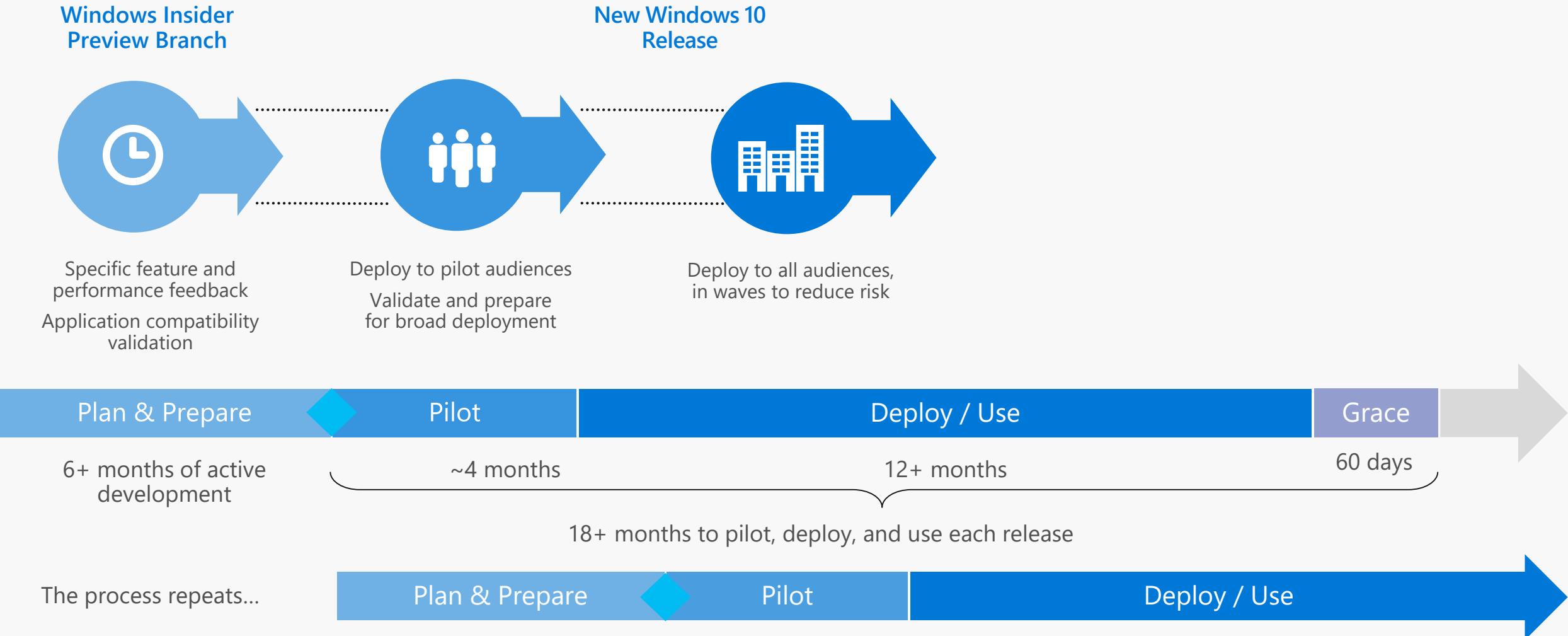
*Conceptual illustration only

Windows as a service: Deploying Windows



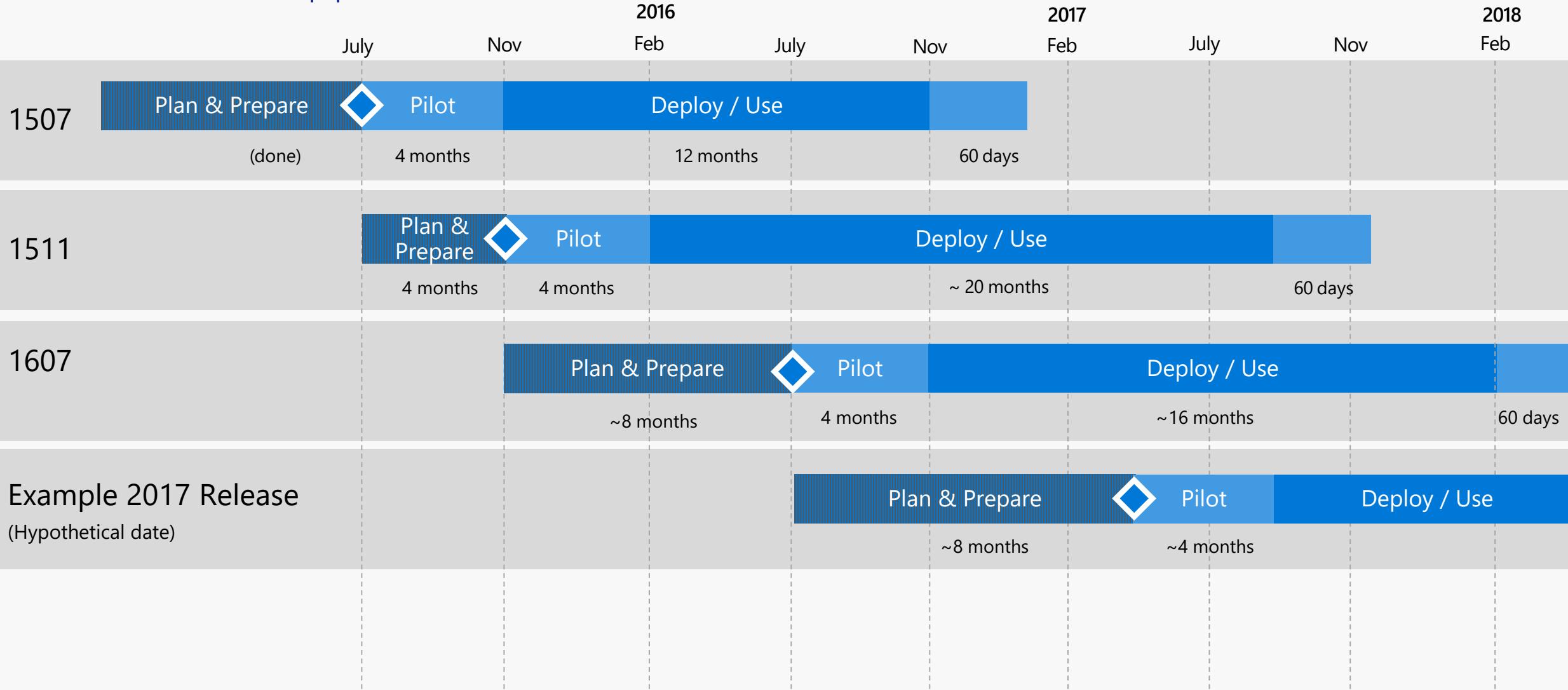
*Conceptual illustration only

Windows as a service: timelines



Windows as a service: Establishing a rhythm

Two releases supported in market



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	✓	
1 st party browsing choices	Microsoft Edge, IE 11	IE 11
Support for Universal Office and some 1 st 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

Transform Pro to Enterprise

Bulk Upgrade from WU

Bulk upgrade using media

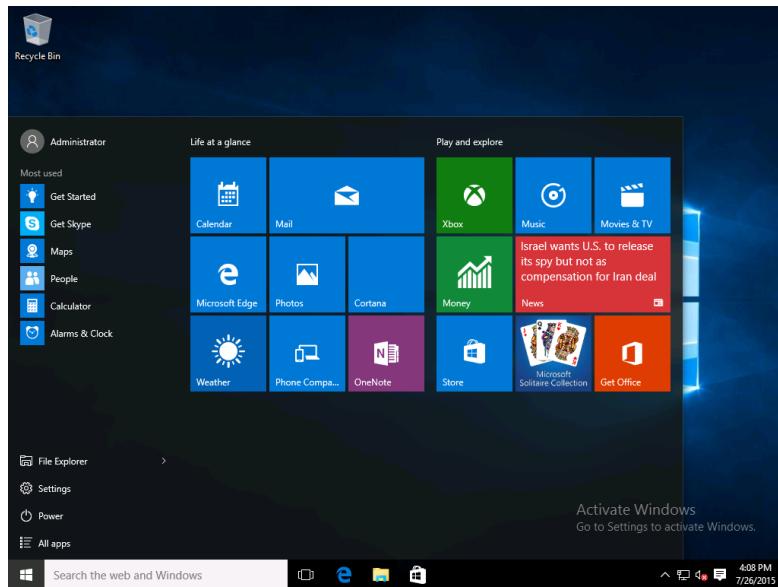
Current Branch for Business (CBB)



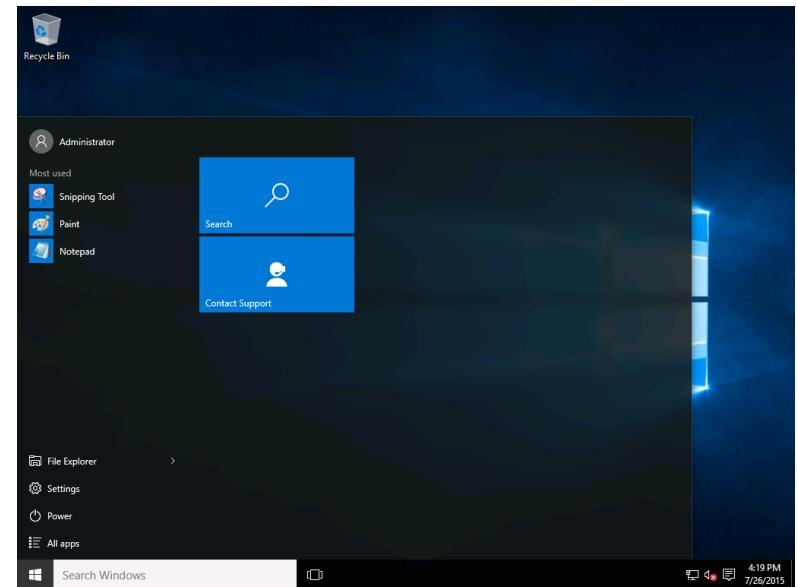
Pro only



Long Term Servicing Branch (LTSB)

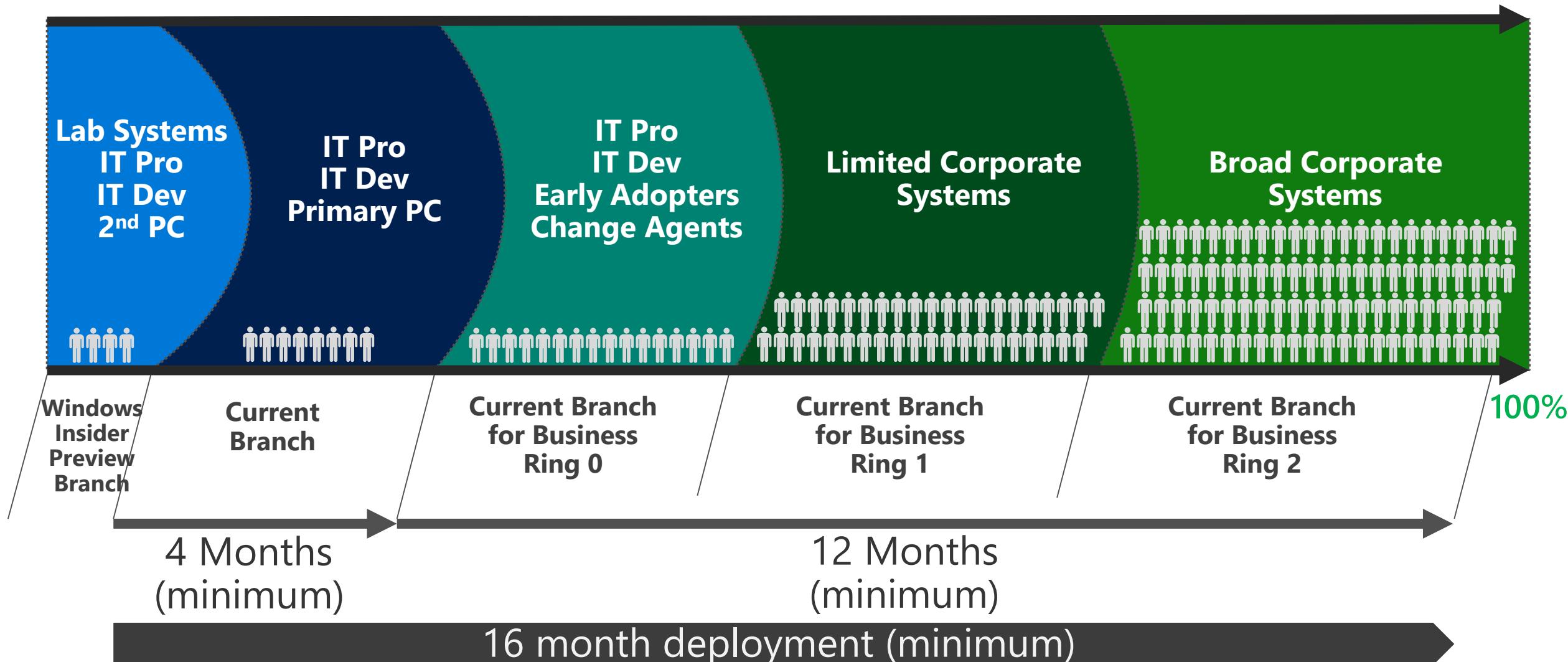


Microsoft Windows 10 Enterprise

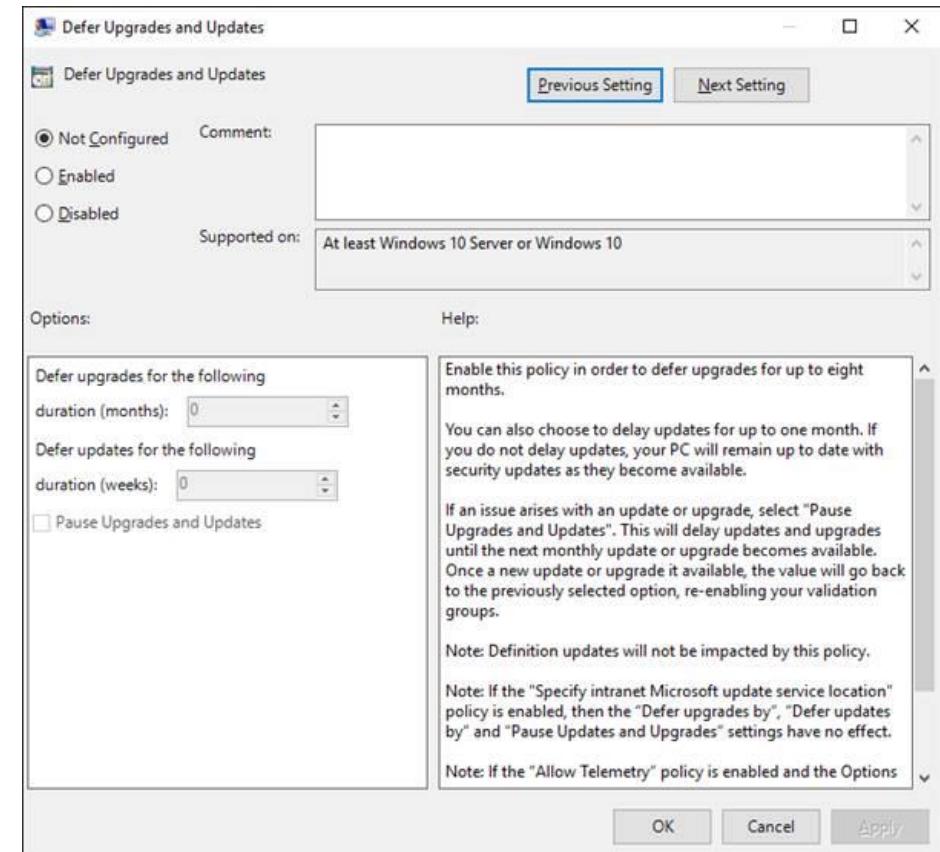
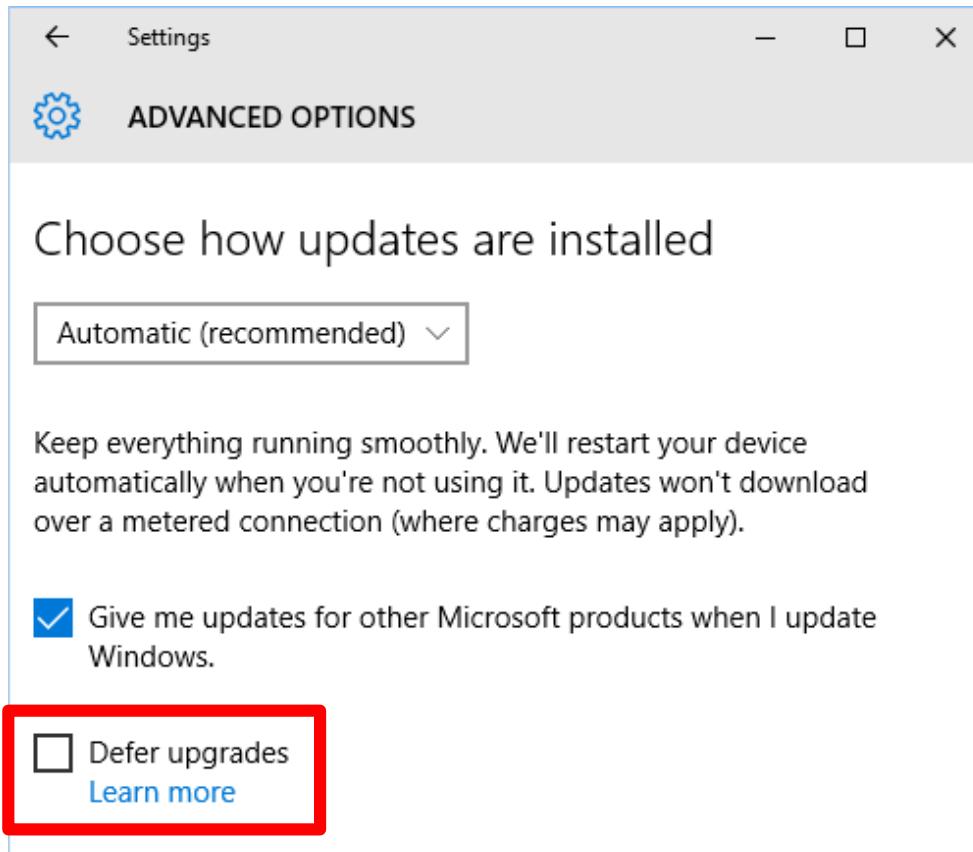


Microsoft Windows 10 Enterprise 2015 LTSB

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.

Windows 10: Specifying a preference for what comes next

Devices are not considered CB or CBB

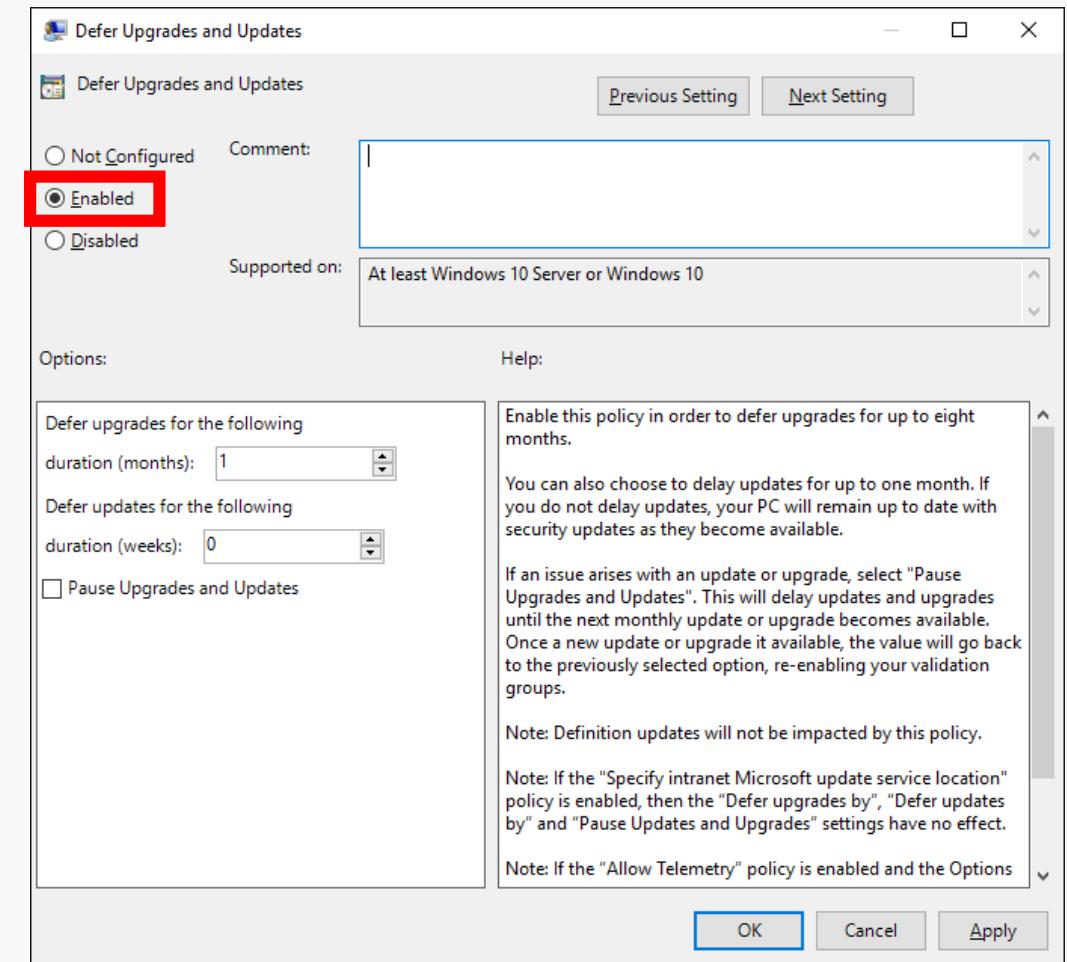
Windows 10 releases transition from one stage to the next

Starts as Current Branch, progresses to Current Branch for Business

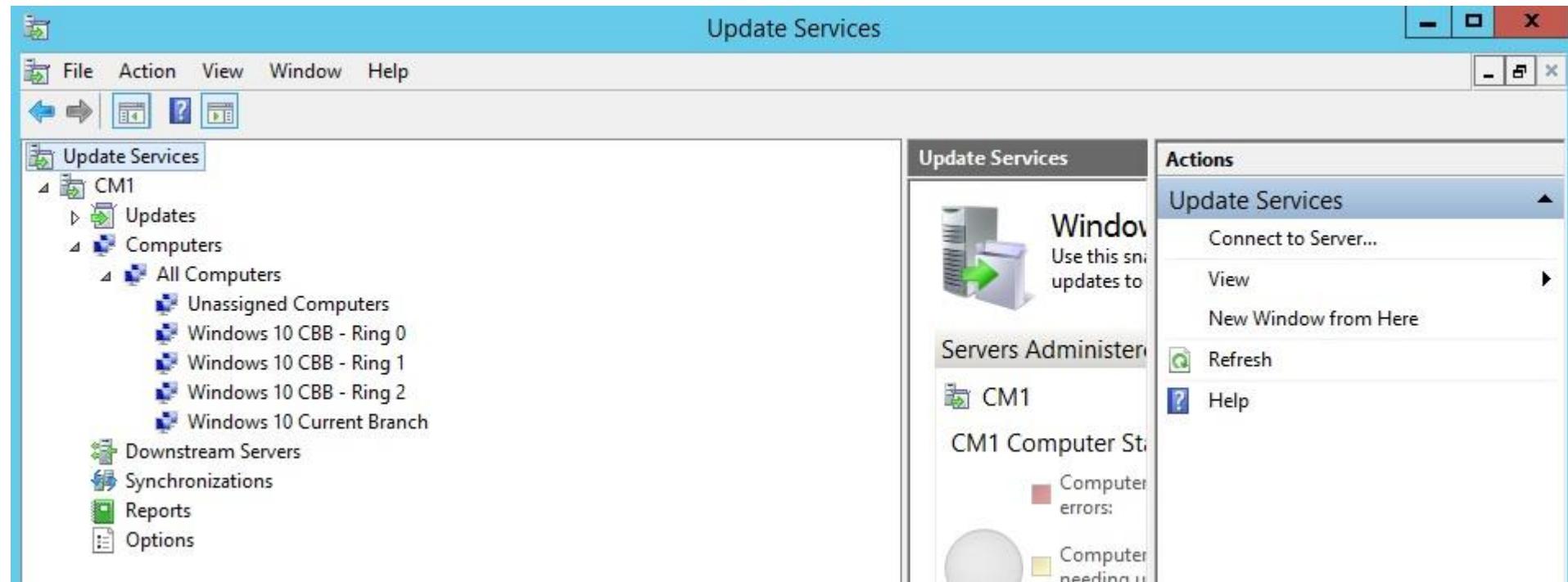
Devices specify when they prefer to move to the next feature update

Specify to "Defer" when you want to wait for Current Branch for Business

Each deployment or management tool can implement this idea differently



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

Upgrade process: Dynamic Update

Dynamic Update does useful things:

- Grabs the latest servicing update to inject on the fly into the media (mounts install.wim copy locally, injects cumulative update) – even if you've manually done this
- Gets any needed drivers that aren't in the media
- Updates compatibility database

This doesn't work well/at all with ConfigMgr or WSUS today

- Not easy to get needed content onto WSUS (to pull from WSUS instead of WU)
- No obvious way to get Setup to use the content even if it were there
- Still some work to do

Upgrade process: Size

Challenges:

- Each feature update is 3.5GB per PC (whether from Windows 7/8.1 or from Windows 10 to a later feature upgrade)
- Each monthly quality update is now up to 1GB per PC, when using ConfigMgr or third-party patching tools

Recommendations:

- Peer to peer distribution
- Use of Express updates (with WSUS), reduces monthly traffic to 100MB per month
- Future differential upgrade support

Express Updates with Other Tools

Requires Windows 10 changes

- Will be enabled for Windows 10 1607 and Windows 10 Enterprise LTSB 2016 (and beyond)
- Enables management and patching tools to leverage express updates
- Windows changes due in **Q1 2017**
- Delivered as part of a cumulative update

Requires tool changes

- Support to be added to **System Center Configuration Manager 1610** release
- New Windows capabilities being documented for use by any management or patching tool
- Contact the tool ISV for details on their implementation plans and timelines

Will reduce network traffic by an **order of magnitude!**

Feature Updates

Expected two to three times per year

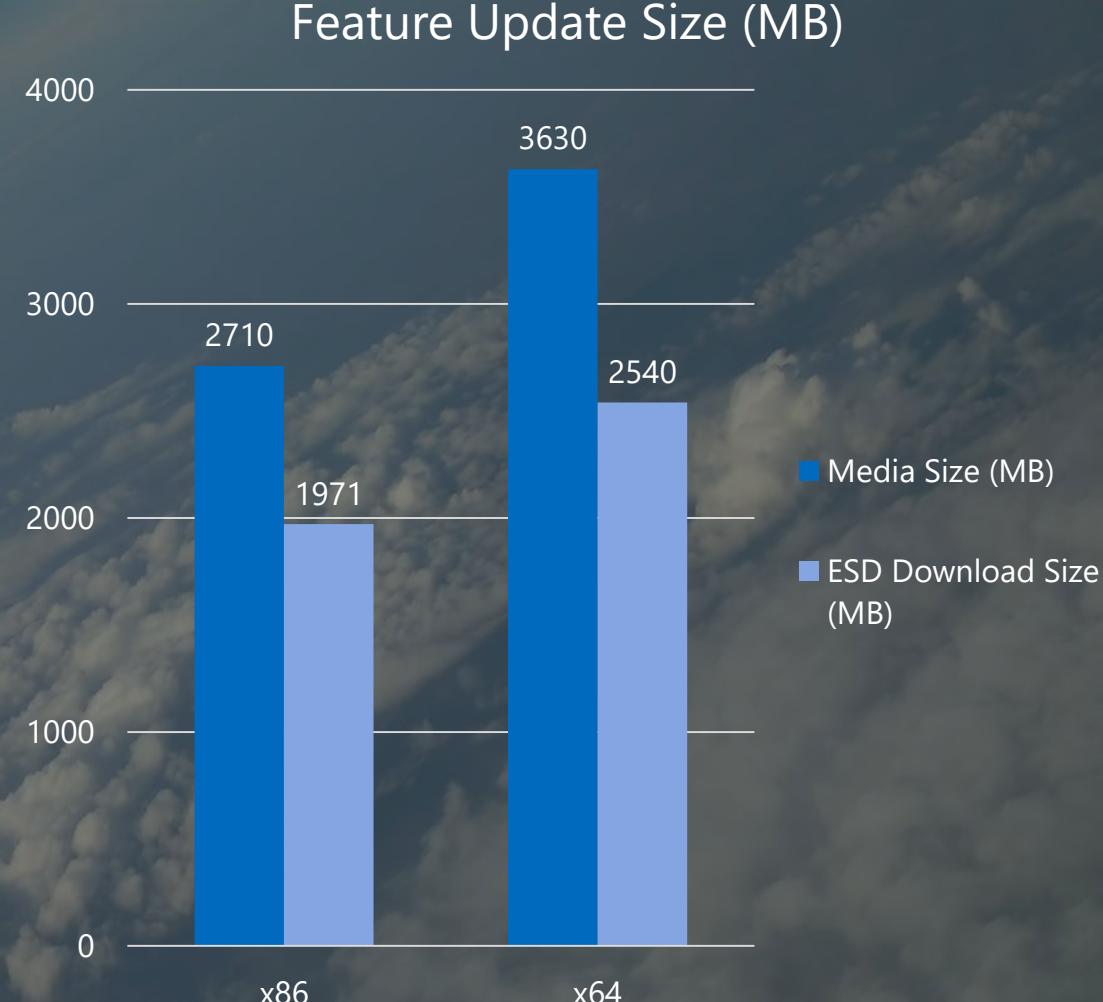
- Minimum of 18 months of servicing for each release, longer when releases are farther apart
- Deployed over an extended period of time, allowing traffic to be spread out (unlike quality updates which often have short deadlines)

Complete set of operating system files

- ESD files are about 30% smaller!
- Highly recommended to use ESD files (provided by WU or WSUS) instead of media (through ISOs)

Deployed like an update, performs an in-place upgrade

- Takes 30-90 minutes, depending on hardware



Feature Updates

Planned Enhancements

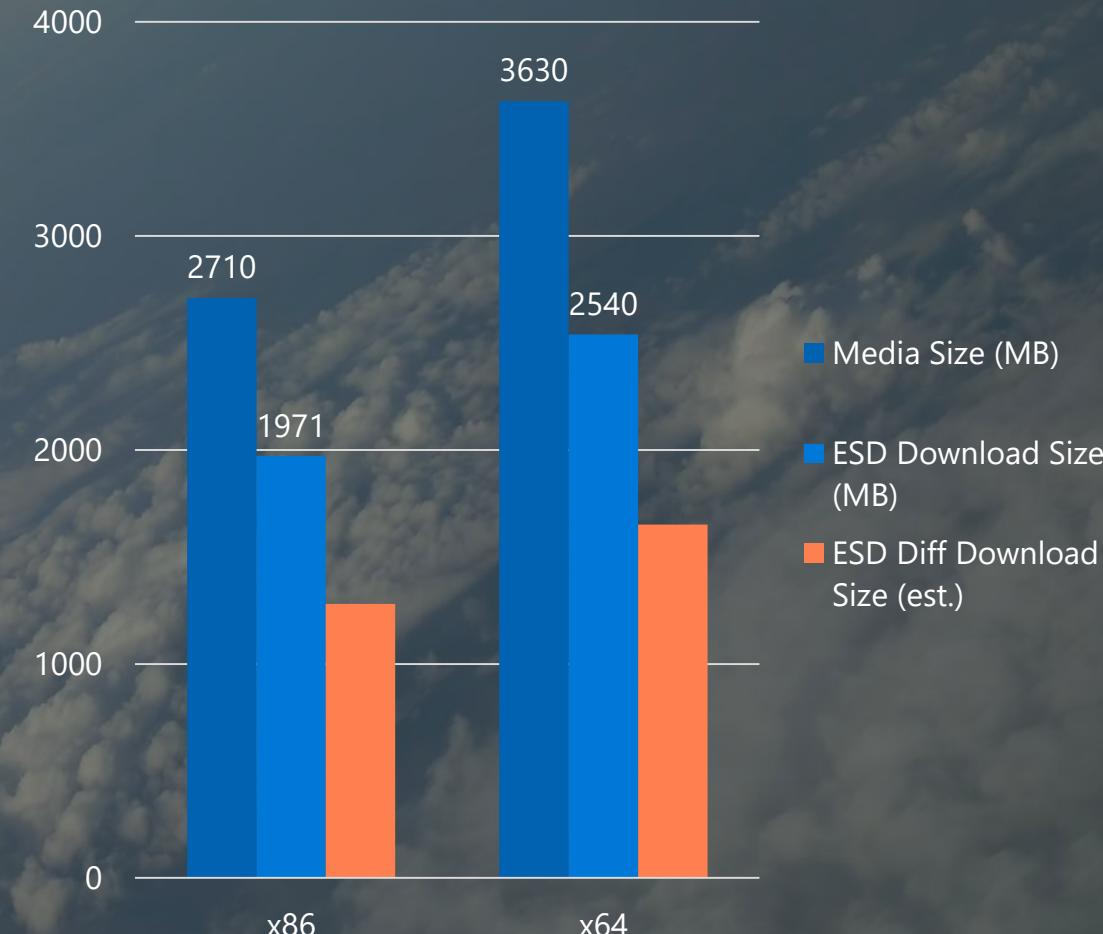
Support for differential upgrades

- Determine what files have changed, then only download those
- Potential **savings of about 35%** over current ESD sizes
- Targeting the feature update planned for **later in 2017**
- Management and patching tools will need to be updated to support this new capability

End user experience is unchanged

- Deployed like an update, performs an in-place upgrade
- Takes 30-90 minutes, depending on hardware

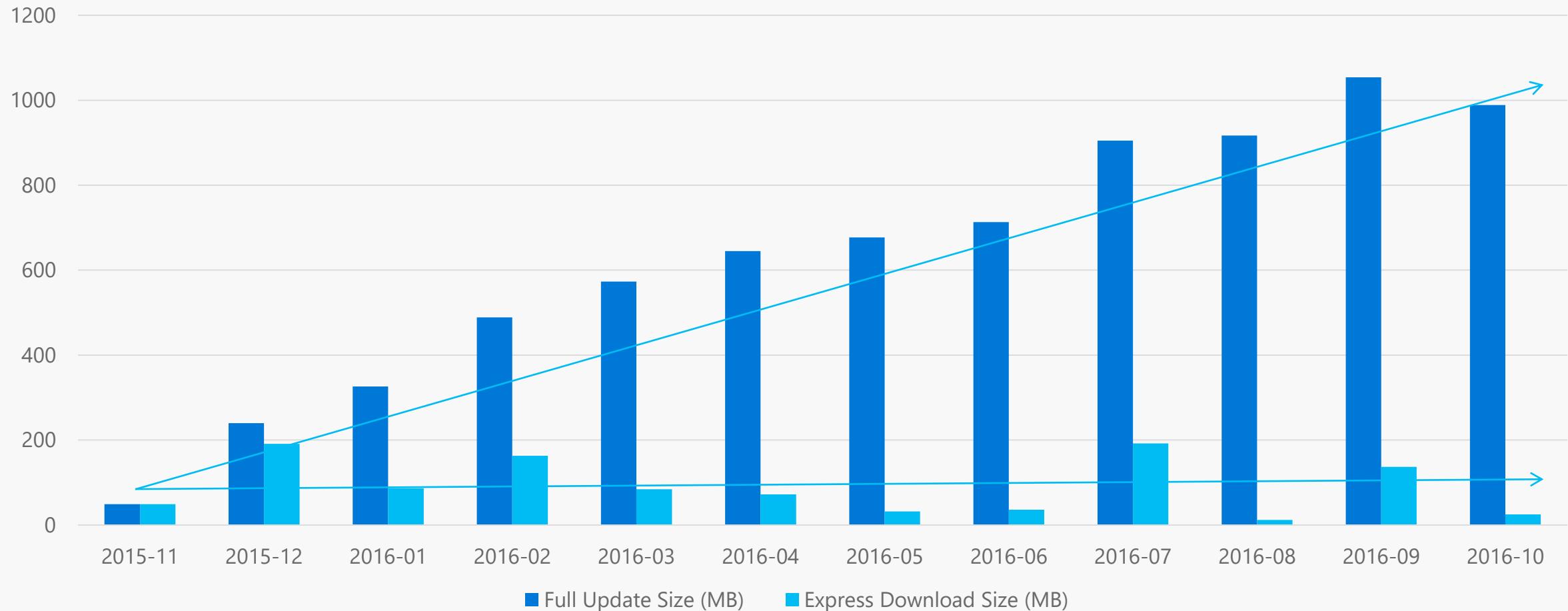
Feature Update Size (MB)



Note: Percentage savings are estimated and can vary due to many factors.

Windows 10 Quality Updates

Express Download Size



Identifying a tool to use

Windows Update

Cloud

Upgrades installed as they
are released (subject to
throttling)

Delivery optimization for
peer-to-peer distribution

Only option for Windows
10 Home

Windows Update for Business

Cloud

Upgrades can be deferred
Builds on top of Windows
Update

Uses Windows Update for
content

Windows Server Update Services

On-Prem

Upgrades are deployed
when you approve them

Content distributed from
WSUS servers

Requires KB3095113
BranchCache to reduce
bandwidth

System Center Configuration Manager

On-Prem

Choice of task sequence-
based upgrades or (with
vNext) software update
capabilities

Content distributed from
ConfigMgr DPs

BranchCache to reduce
bandwidth

Distributing content using peer-to-peer

The server and data center are bottlenecks

The edges of the network have more capacity

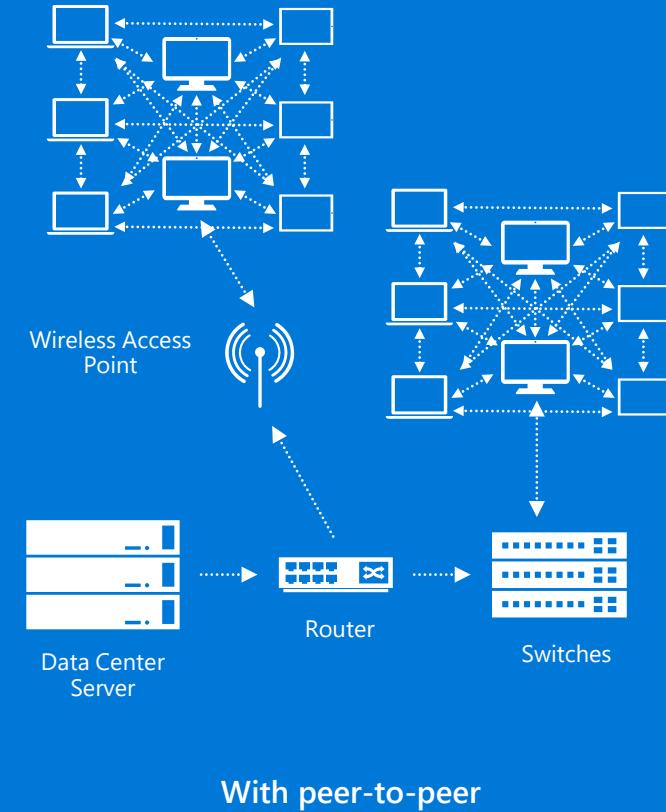
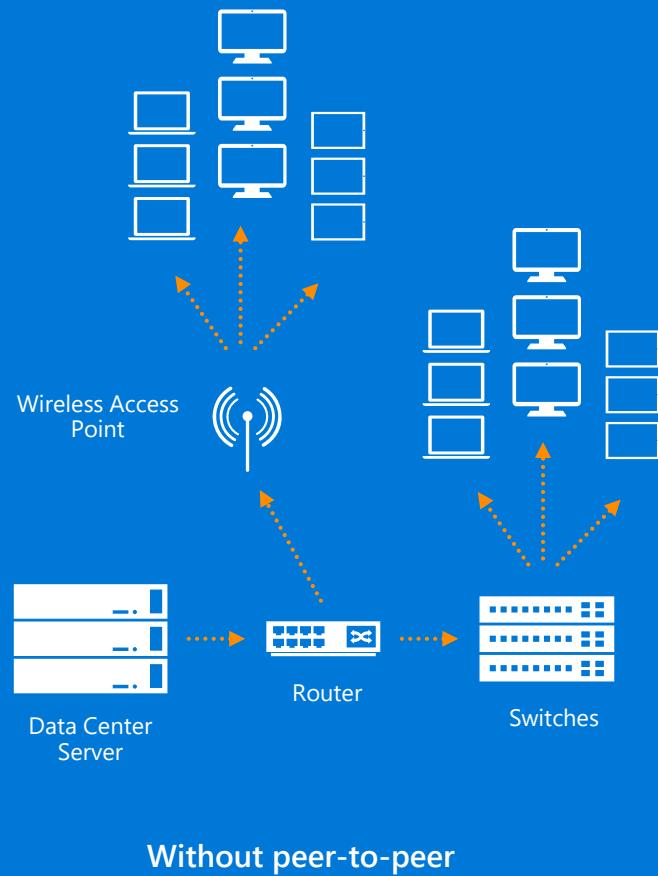
Using peer-to-peer technologies shifts the traffic to the edges

- BranchCache (with WSUS, ConfigMgr)
- Delivery Optimization (with WU, WU for Business)

90% or more of the traffic can be shifted

Simple to implement, great for large and small offices

Immediate return on investment



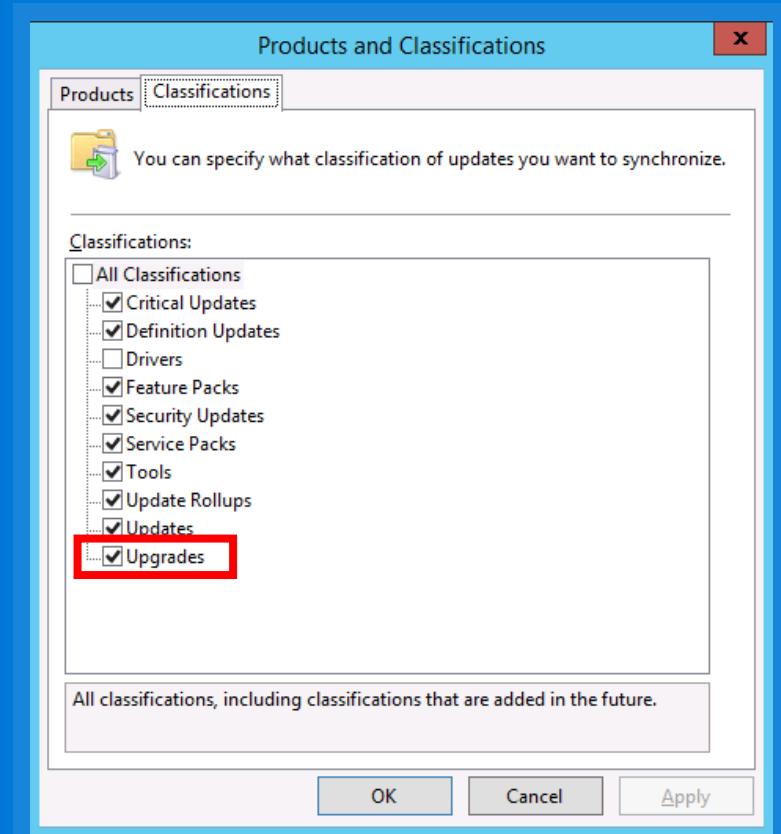
Windows Server Update Services

Updated to support Windows 10 feature upgrades, including upgrades from downlevel OSes

- Requires WSUS 4.0 (Windows Server 2012 or above) with KB3095113
- See <http://blogs.technet.com/b/wsus/archive/2015/12/04/important-update-for-wsus-4-0-kb-3095113.aspx> for an important note

Windows 10 1607 CBB published on 1/19

Enabling upgrades



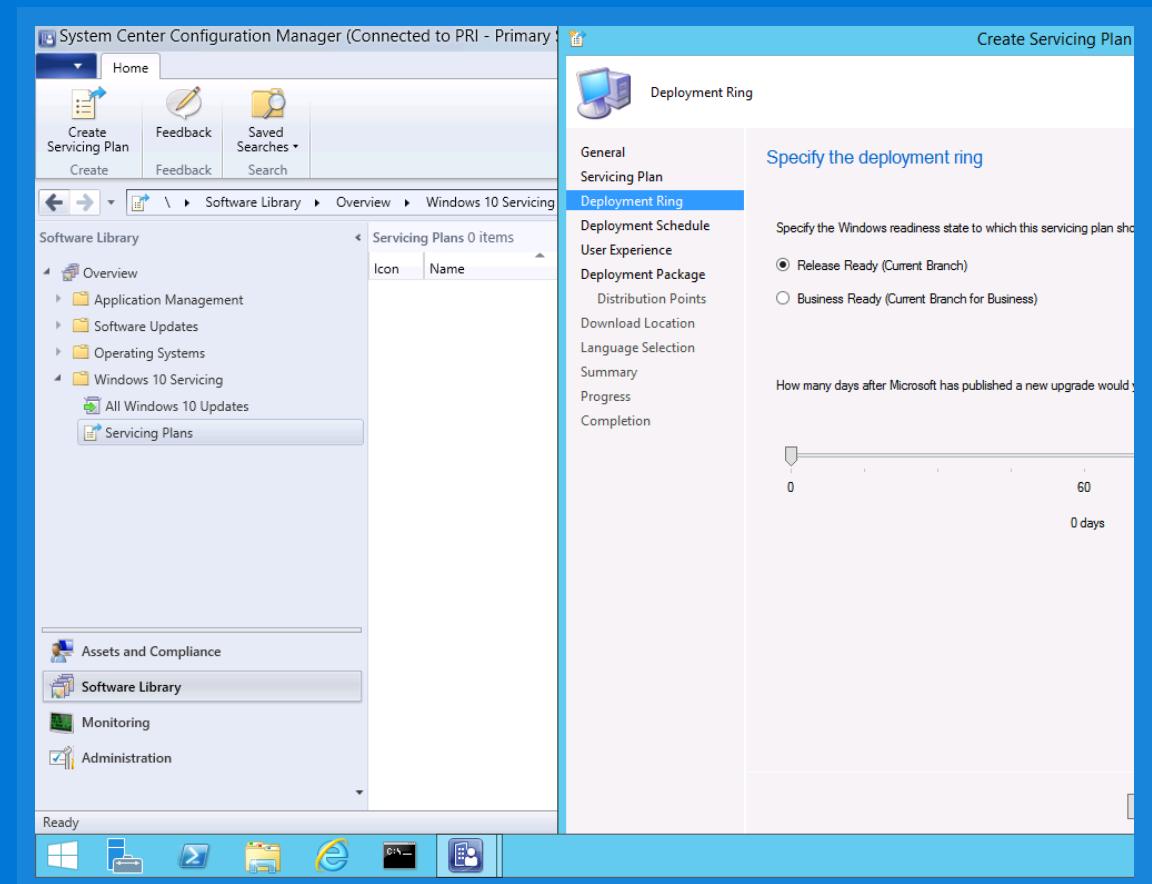
System Center Configuration Manager

System Center Configuration Manager
1602 or later needed to support Windows
10 1607

- Requires WSUS 4.0 (Windows Server 2012 or above)
with KB3095113

Windows 10 Servicing Plans provide
automation

Servicing Plans



Compatibility in Windows 10

Outstanding compatibility means a smooth migration from Windows 7 or Windows 8.1

Desktop apps

Organizations are observing compatibility rates above 99%

High compatibility achieved through:

- Minimal changes to Win32 APIs
- Insider feedback during development
- Telemetry

Web sites

Internet Explorer 11 included (unchanged) for backwards compatibility

New Microsoft Edge browser for modern HTML5-based web sites

Enterprise Mode features to ensure proper use

Modern apps

High compatibility achieved through:

- Validation of Windows Store apps
- Insider feedback during development
- Telemetry

Significant investments, enhancements in each release

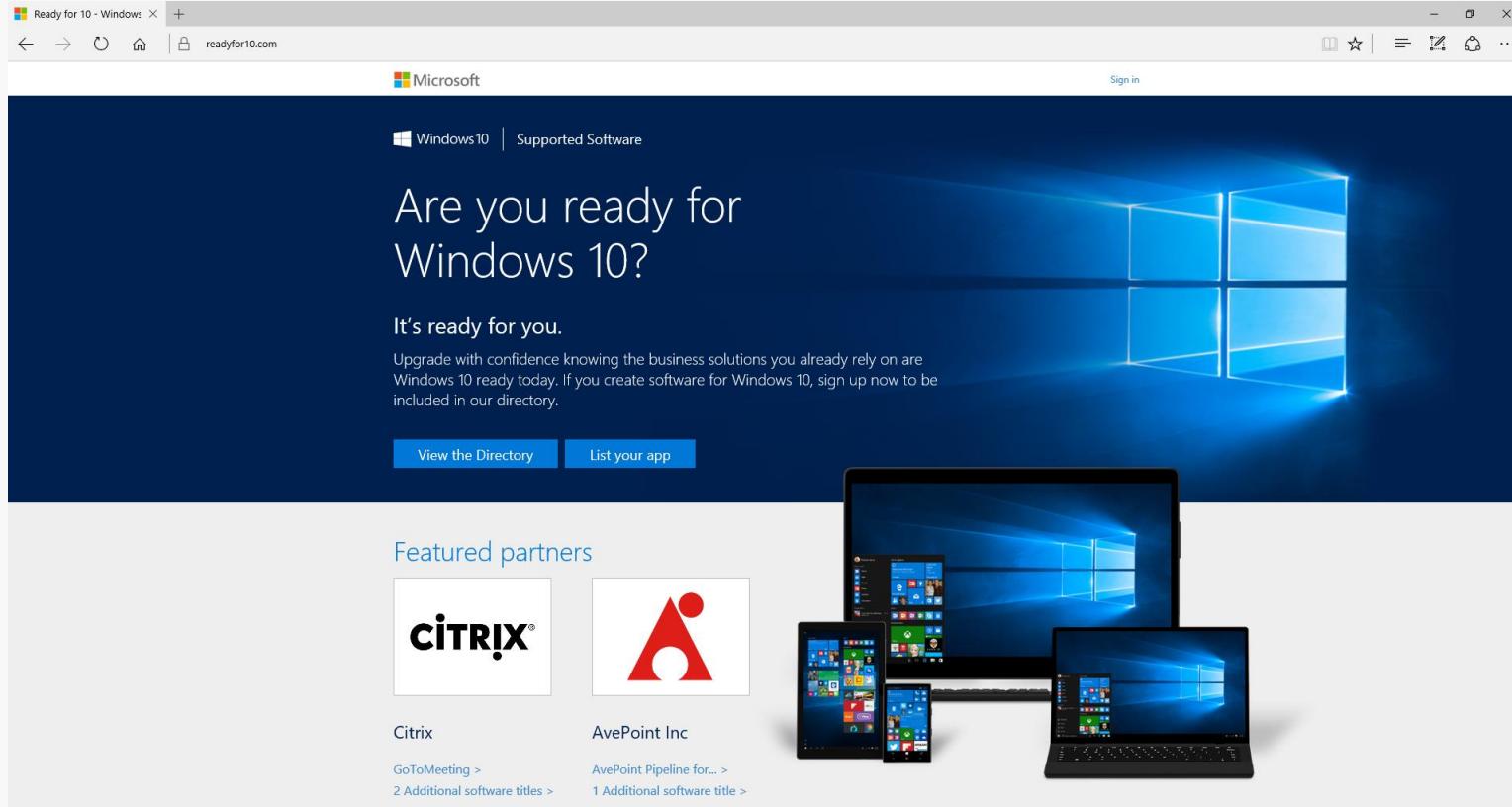
Hardware

Windows 10 supports all devices capable of running Windows 7 and above

Identical hardware minimum requirements as Windows 7

Strong driver compatibility, with updates delivered as needed through Windows Update

Compatibility in Windows 10



Get links to Windows 10 ISV support statements

<http://www.readyforwindows.com>

We are actively engaged with ISVs, to ensure full support for Windows as a service

How to validate applications

Create and maintain an app portfolio

Complete list of apps and web pages used throughout the organization

Business and IT experts identified

IT works with the business to eliminate duplicates, define supported versions



Prioritize, identifying critical apps

Business critical
Managed
Supported
Unsupported
Blocked



Validate business-critical apps

Structured testing, using predefined test plans executed with business and IT experts
Automated if possible
Target small percentage of apps



Leverage pilots for broader validation

IT pilot, to gauge infrastructure, environment, and business productivity app readiness

Business pilot, targeting the broadest set of applications possible

Broad deployment using rings, to minimize risk

Coming soon: Windows Upgrade Analytics

Track upgrade readiness

Leverage telemetry to see what's happening in your organization

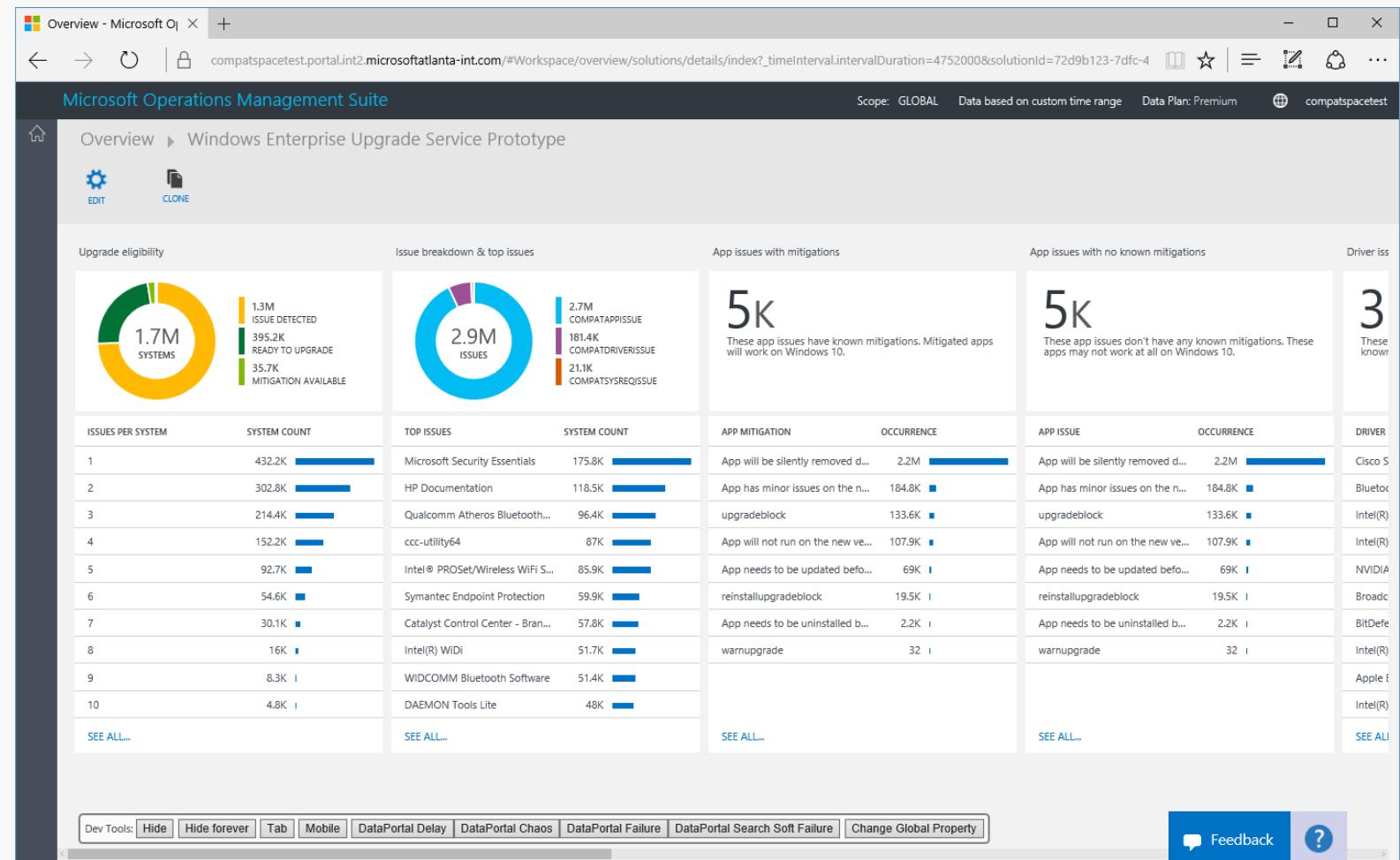
Identify app and driver issues

See app and device details, known issues

Remediate

Implement suggestions to resolve issues

Drive deployment



Sign up via <http://www.microsoft.com/en-us/WindowsForBusiness/upgrade-analytics>

Overview - Microsoft O| X +

compatteamstudygroup.portal.mms.microsoft.com/?returnUrl=%2F#Workspace/overview/solutions/details/index?solutio

Microsoft Operations Management Suite Data based on custom time range

Ask me anything

Microsoft Ignite

Upgrade Analytics

UPGRADE OVERVIEW

13K Total computers

5 Computers upgraded

Last updated 09/28/2016 at 06:00 PM

OVERVIEW COUNT

Total computers	13K
Computers upgraded	5
Total applications	54K
User changes	Data refresh pending

RUN A PILOT

Computers with no system or application issues known to Microsoft. Attention may be needed to resolve driver issues before starting a pilot project.

4K

COMPUTER ASSESSMENT COMPUTER COUNT

OK to pilot, fixed during upgrade	2.5K
No known issues	1.4K

PRIORITIZE APPLICATIONS

54K Total applications

5 Applications included with

IMPORTANCE
Low install count
Not reviewed
Business critical
Ignore
Important

Prepare your environment

More info

Upgrade overview

Inventory of computers and applications sharing upgrade readiness information with Microsoft. Data changes are refreshed daily so you can monitor upgrade readiness status.

Run a pilot

Computers with no issues known to Microsoft. Select the computers you want to use in a pilot and then export this list to your software distribution solution.

Prioritize applications

Assign importance levels to prioritize the applications you plan to test and validate. Applications installed on 2% or

9:37 AM
9/29/2016

Windows 10 1607: Important Dates

- Released as CB on 8/2.
- CBB announced on 11/29 (about four months later).
- Windows Update and WSUS feature update packages (used by ConfigMgr's Windows 10 servicing plans) updated on 1/19.
- Updated media available on VLSC on 1/26.
 - 60-day grace period on Windows 10 1507 starts on 1/26.
- Windows 10 Enterprise LTSB 2016 needs new keys and KMS hotfixes; the CB release does not.
 - First install KB 3058168 (Activate Windows 10 from WS 2012/2012 R2 KMS Hosts)
 - For Windows Server 2012, then install KB 3172615. For Windows Server 2012 R2, then install KB 3172614

Die vier Phasen des Upgrade Prozesses

1) Down-level

Herunterladen von Updates

Fehlerprüfung des aktuellen OS

C:\\$Windows.~BT

Kompatibilitätsprüfung

Analyse der OS Komponenten

Inventory der Applikationen

Inventory der Treiber

Vorbereiten des WinRE

2) WinRE

Boot in ein minimalistisches OS

Beide Betriebssysteme sind offline

Backup des alten OS

Vorbereiten des neuen OS

Install.wim ->
\$WINDOWS.~BT\NewOS

3) 1st boot to new OS

Start bei "Specialize"

Installieren der Treiber

Konfiguration der Windows Apps

Konfiguration des WinRE

Ausführen von Bereitstellungspaketen

Installation von Windows Features

Teilweise Wiederherstellung von
Daten und Einstellungen

4) 2nd boot to new OS

Start bei "OOBE"

Welcome Schritte werden
durchgeführt

Finalisieren des Upgrades

(Cortana, Standard Fotos, Musik,
Video und Internet Explorer)

Ready

Set

Go

Welcome to Windows 10

Wiederherstellung möglich?

1) Down-level

Clean up der gesammelten
Daten

2) WinRE

Reboot in Ursprungsbetriebssystem
Clean up der gesammelten Daten

3) 1st boot to new OS

- Reboot in Windows Recovery Environment (WinRE)
- Alle Files und Ordner vom "System-" laufwerk werden entfernt
- Verschieben der Dateien und Ordner aus Windows.Old in die ursprüngliche Lokation
- Cleanup der gesammelten Daten
- Reboot ins Original OS

4) 2nd boot to new OS



Welcome to old Windows

Cleanup

Restore

Ready

Recovery möglich?

The screenshot shows the Windows Settings app open to the 'Update & Security' section. On the left, a sidebar lists several options: Windows Update, Windows Defender, Backup, Recovery (which is highlighted with a blue bar), Activation, and For developers. To the right, there are three main sections: 'Reset this PC', 'Go back to Windows 7', and 'Advanced startup'. Each section has a descriptive text block and a 'Get started' button. A red box highlights the 'Go back to Windows 7' section.

← Settings

UPDATE & SECURITY

Windows Update

Windows Defender

Backup

Recovery

Activation

For developers

Reset this PC

If your PC isn't running well, resetting it might help. This lets you choose to keep your files or remove them, and then reinstalls Windows.

Get started

Go back to Windows 7

This option is only available for a month after you upgrade to Windows 10.

Get started

Advanced startup

Start up from a device or disc (such as a USB drive or DVD), change Windows startup settings, or restore Windows from a system image. This will restart your PC.

Restart now

Upgrade: When not to use

In some scenarios for upgrading from Windows 7 or Windows 8.1

- Changing from Windows x86 to x64
- Systems using Windows To Go, Boot from VHD
- ~~Changing from legacy BIOS to UEFI~~
- Dual boot and multi-boot systems
- ~~Image creation processes (can't sysprep after upgrade)~~
- Using some third-party disk encryption products

Upgrade: Third-Party Disk Encryption

With Windows 10 1511 or 1507, you could inject third-party disk encryption software into media images

- Mount boot.wim, install.wim
- Follow vendor-provided instructions

With Windows 10 1607, a new process works with media and ESD-based scenarios (WSUS, WU/WUfB, ConfigMgr servicing)

- Place needed files (driver INF, supporting files) in a folder on the PC
- New Setup.exe /ReflectDrivers switch allows you to specify driver files that Setup should inject into the media
- For ESD-based scenarios, place a SetupConfig.ini file on the machine where Setup can find it:

```
%systemdrive%\Users\Default\AppData\Local\Microsoft\Windows\WSUS\SetupConfig.ini
```

BitLocker is so much easier

Upgrade: Languages

System UI language of the running OS must match that of the image being used to upgrade

- You can change the system UI language in the OS or in the image to make it match, e.g. "Dism /image:E:\ /Set-UILang:en-US", but only offline
- Certainly supported to modify the image offline, no clear answer on modifying the running OS offline

Additional language packs must be reinstalled after the upgrade – you can provide a set of them to SETUP and it will take care of it

- With media-based approaches, use Setup.exe with /InstallLangPacks switch, pointing to a folder with the language pack files (a few per language)
- With ESD-based approaches, use the same approach but with the SetupConfig.ini file

Challenges:

- Identifying what languages are needed for each PC (if they are different)

Upgrade process: Drivers

Some classes of drivers are not migrated forward

- Display and Bluetooth drivers are left behind, as well as any driver considered incompatible

If other drivers are needed, provide them to Setup

- Create a folder with the needed drivers
- With media, specify Setup.exe /InstallDrivers pointing to that folder
- With ESD-based scenarios, use a SetupConfig.ini file
- Understand driver ranking rules for installation

Upgrade process: In-Box Apps

Customers can remove in-box apps, but each feature update puts them back

- See <https://blogs.technet.microsoft.com/mniehaus/2015/11/11/removing-windows-10-in-box-apps-during-a-task-sequence/> for removal

Workarounds:

- Remove them again post-upgrade
- Remove them from the install.wim before upgrading (only works for media-based scenarios, e.g. task sequences)
- See <https://blogs.technet.microsoft.com/mniehaus/2016/08/23/windows-10-1607-keeping-apps-from-coming-back-when-deploying-the-feature-update> for details

Future feature updates will provide better solutions

- Windows 10 Creators Update will keep user-uninstalled apps from coming back
- The next feature update after that will keep IT-removed (de-provisioned) apps from coming back

Upgrade process: Settings Migration

The upgrade process should migrate all settings

- Default applications (file associations)
- User, system, and app settings

Some settings may not be migrated properly

- These should be considered bugs – we want this process to be seamless
- Open cases with Microsoft support to investigate, work with your TAM to submit feedback

Upgrade process: Preflight

Determine ahead of time if the upgrade will succeed

- Use SETUP.EXE /Auto Upgrade /Compat ScanOnly /Quiet
- Check the return codes, XML files
- Requires the full media (including WIM files), so don't download and execute

For more information:

- <http://blogs.technet.com/b/mniehaus/archive/2015/08/23/windows-10-pre-upgrade-validation-using-setup-exe.aspx>

Upgrade process: BIOS to UEFI

New tool expected with the Windows 10 Creators Update

- MBR2GPT.EXE enables in-place conversion of an existing disk
- Can be done as part of the deployment (e.g. wipe/load) or after (e.g. post-upgrade)
- Still requires the use of OEM firmware configuration utilities to reconfigure the firmware, enable Secure Boot

Upgrade process: Other notes

New Active Hours policy

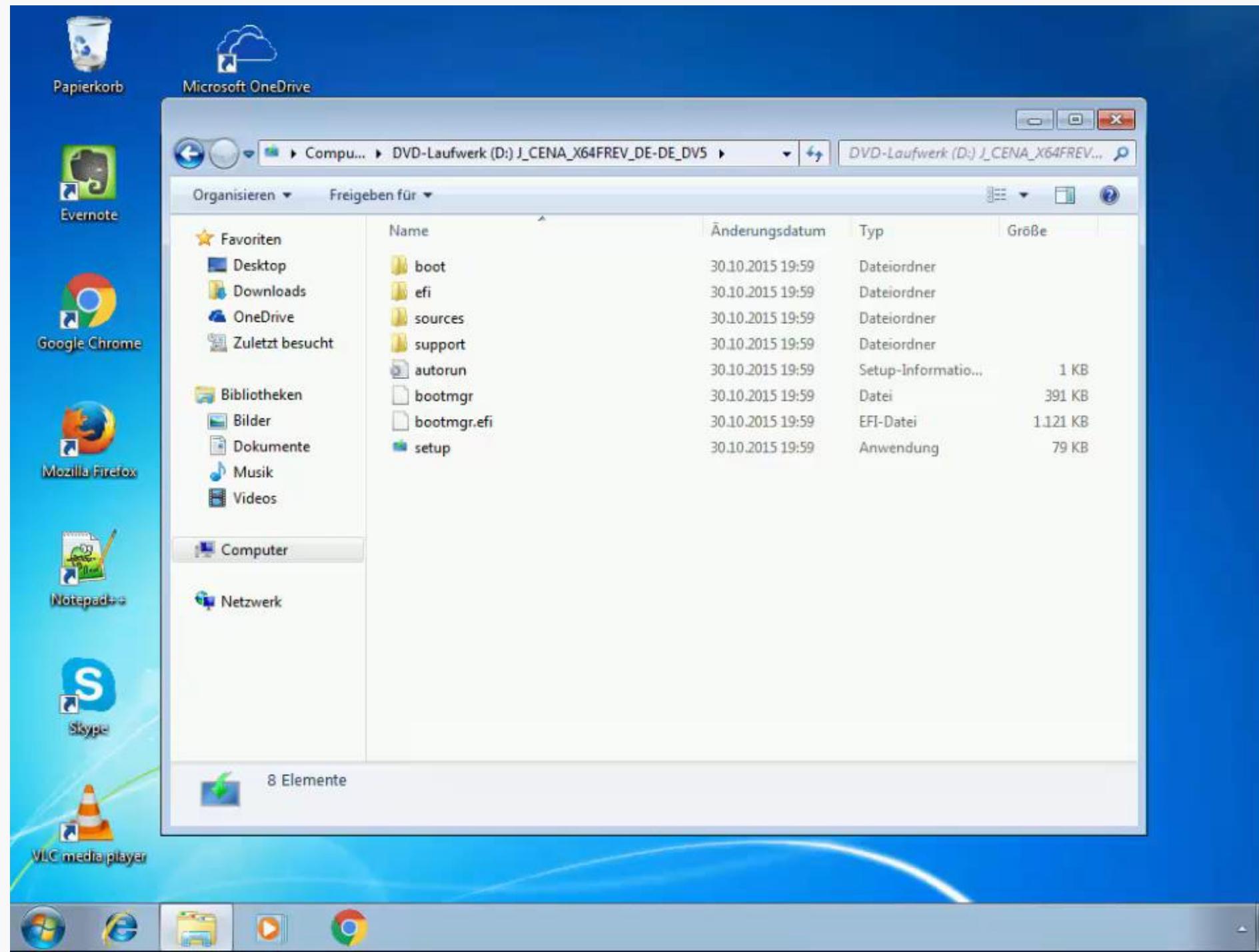
- Quality updates and feature updates won't be installed by WU agent (WU, WUfB, WSUS) during time window configured

New Windows Update for Business Policies

- New settings work only with Windows 10 1607 (for future updates after 1607 is installed); old policies only work with Windows 10 1511
- Feature updates can be deferred for 1-180 days, quality updates by 1-30 days
- Support for deferrals for both CB and CBB

Delivery Optimization is used with WSUS

- Windows Update agent in Windows 10 1511 and 1607 will check in with Delivery Optimization service to try to do peer-to-peer transfers, then fall back to getting content from WSUS
- Can be configured via Delivery Optimization policy to instead just use BITS (great for BranchCache peer-to-peer)
- See <https://blogs.technet.microsoft.com/mniehaus/2016/08/16/windows-10-delivery-optimization-and-wsus-take-2/> for more detail



Microsoft IT Camps – Windows 10 Enterprise Deployment

AGENDA

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

Windows 10 Deployment Stack & Supporting Technologies

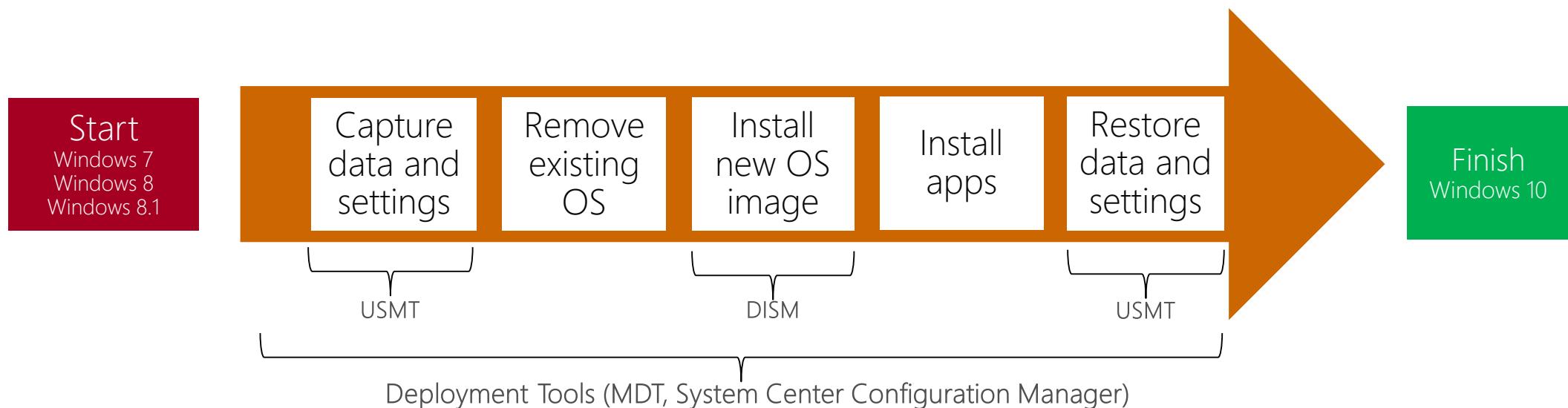
	Image	Wipe & Load	In-Place Upgrade
Cloud	Windows Update	Windows Update	Windows Update
	Windows 10 Media	Azure Active Directory	Azure Active Directory
Windows 10 Enterprise Device	Architecture	User State	User State
	Computer Policy	Drivers	Compatibility Checker
On-Premises	Branding	Start Screen & Taskbar Customization	Start Screen & Taskbar Customization
	Start Screen & Taskbar Customization	Computer Policy	Computer Policy
Microsoft Deployment Toolkit		Microsoft Deployment Toolkit	Microsoft Deployment Toolkit
Security Baseline (Optional)		Active Directory	Active Directory
Windows Server Update Services	Windows Server Update Services	Software Update Point (Server 2008 R2 & above)	Software Update Point (Server 2012 & above)
	Active Directory	Distribution Point	Distribution Point
System Center Configuration Manager (Current Branch)			

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	<ul style="list-style-type: none">▪ No infrastructure required to deploy▪ Support Challenges▪ Challenging to maintain versioning	<ul style="list-style-type: none">▪ Remote offices▪ Limited network connectivity
Lite touch Deployment (LTI)	Microsoft Deployment Toolkit	<ul style="list-style-type: none">▪ Less engineering time than ZTI▪ Requires interaction to initiate the deployment process▪ Varied levels of automation supported	<ul style="list-style-type: none">▪ Windows 10 Pilot▪ Interactive deployment capability
Zero Touch Deployment (ZTI)		<ul style="list-style-type: none">▪ Requires the most engineering time▪ No user interaction required to initiate deployment▪ 100% automation	<ul style="list-style-type: none">▪ 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



Firmware



- Flexible Deployment Media Support
- All legacy deployment methods still apply
- Maintain a single boot image

Device Examples

Devices purchased over 4 years ago

- 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



*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	<ul style="list-style-type: none">▪ Easy to setup and maintain.▪ Driver to client device matching 'just works'	<ul style="list-style-type: none">▪ Less control over drivers chosen – first driver wins.▪ If a problem occurs, troubleshooting is more difficult.
Apply Driver Packages (Recommended)	<ul style="list-style-type: none">▪ Administrator can specify the exact driver for a particular make and model of client device.▪ More control over each client device	<ul style="list-style-type: none">▪ Additional up-front configuration and maintenance required.

Assessment and Deployment Kit

New Version Released in August

- Optional, not required to support Windows 10 1607
- Fixes all known issues (including with ConfigMgr)
- USMT adds support for Office 2016

New components added

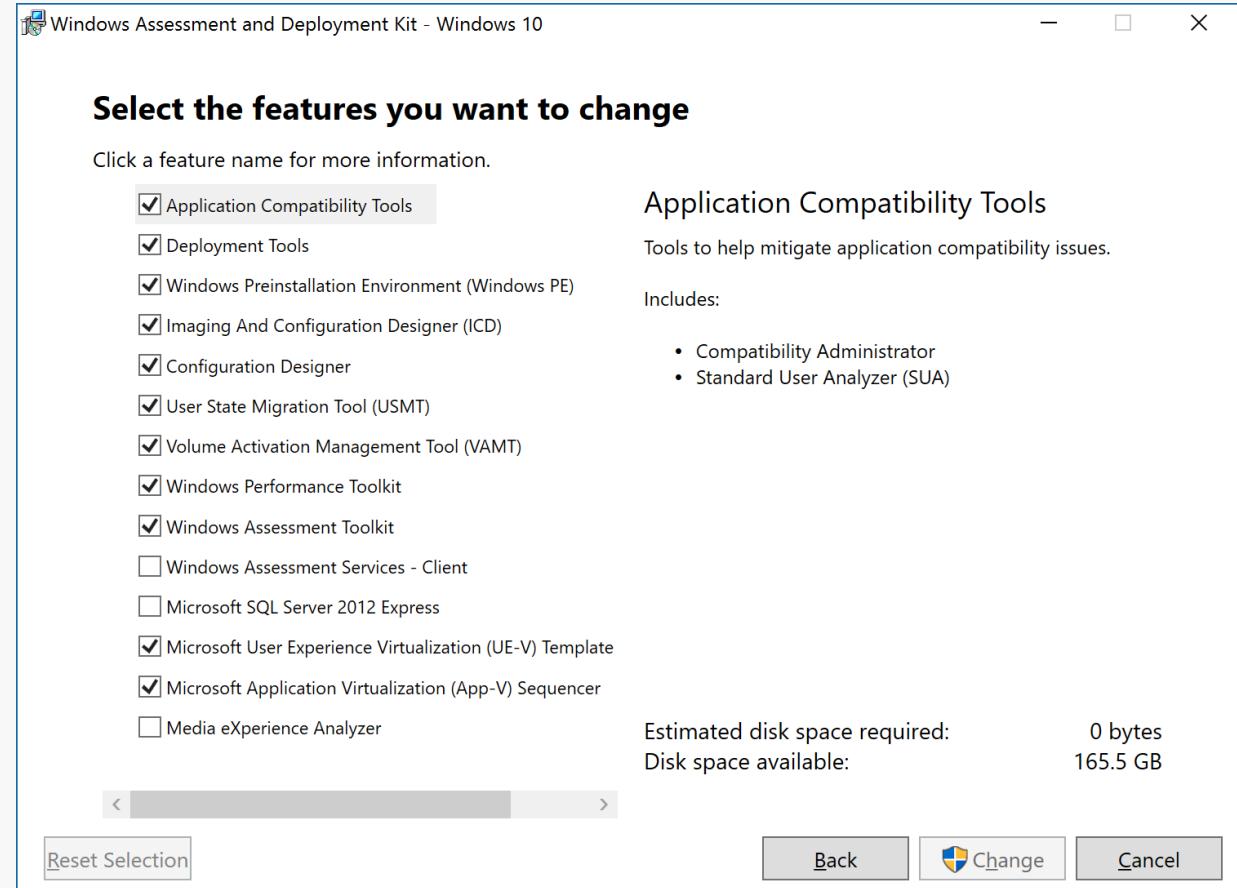
- App-V and UE-V components (features in-box)

Significant updates

- Windows Imaging & Configuration Designer (imaging piece will be removed with the next release)

App Compat Toolkit pieces removed

- Inventory, reporting tools
- Use Windows Upgrade Analytics instead



Microsoft Deployment Toolkit

A new MDT was released on November 14th

- Dropped the year, just uses the build number (8443) for identification
- Mostly bug fixes
- See <https://blogs.technet.microsoft.com/msdeployment/2016/11/14/microsoft-deployment-toolkit-8443-now-available/> for details

New releases will occur as needed

- If necessary to address bugs or compatibility with new Windows releases

For ConfigMgr, the long-term desire is to integrate ZTI and UDI functionality into the product

Configuration Manager

New “current branch” servicing model

- New features added with three releases per year, 12 month support lifecycle for each release
- N-1 support for Windows 10 deployment and management, so ConfigMgr 1602 or 1606 are required to support Windows 10 1607
- Separate technical preview “train”
- See <https://blogs.technet.microsoft.com/enterprisemobility/2016/06/24/faq-system-center-configuration-manager-current-branch/> for details

Two mechanisms for Windows 10 feature updates

- Windows 10 Servicing feature, for automated servicing plans
- Task sequences, when needing to do pre- or post-processing steps or when using customized media

ConfigMgr 1606 Tech Preview deprecates OSDPreserveDriveLetter (and that's a good thing)

- See <https://technet.microsoft.com/en-us/library/mt732696.aspx>

Sysprep changes

Previously, Sysprep did not support upgraded OSes

- For example, upgrading from Windows 7 to Windows 10, then trying to Sysprep and capture would always fail

With Windows 10 1607, Sysprep is now supported on upgraded OSes

- That doesn't mean it's a good idea
- Still recommend using MDT or similar processes to perform an automated build and capture – drop in a new Windows 10 media and go
- Really intended to help customers that aren't sophisticated enough to do this

Taskbar configuration

With Windows 10 1607, you can now configure the task bar

- Add or remove icons, or replace the entire layout
- Driven via Group Policy (same Start screen control policy used for the Start menu) or via LayoutModification.xml file
- Place file in C:\Users\Default\AppData\Local\Microsoft\Windows\Shell

See these links:

- <https://technet.microsoft.com/en-us/itpro/windows/manage/windows-10-start-layout-options-and-policies>
- <https://technet.microsoft.com/en-us/itpro/windows/manage/configure-windows-10-taskbar>

Microsoft IT Camps – Windows 10 Enterprise Deployment

AGENDA

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

Windows Modern Deployment

Quickly prepare new devices for user productivity



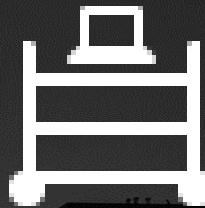
Cloud-Driven

Pre-register devices in the cloud (optional)
Specify e-mail and password
Completely configured with no IT intervention required



Simple, IT-Driven

Use the Windows Configuration Designer to create a package containing customizations
Package copied to each computer, installed to customize the PC



Teacher-Driven

Wizard-driven “Set up School PCs” app to create a USB key with school-specific customizations
Set up additional PCs in just a few minutes using that USB key

- Join the device to the organization
- Enroll the device in a management service

- Configure OS settings
- Install needed apps

Welche Bereitstellungsoptionen gibt es?

Old-school-Methode	In-Place	Provisioning Packages
<ul style="list-style-type: none">• Daten und Einstellungen sammeln• Golden Image• Treiber werden eingespielt• Apps werden eingespielt• Daten und Einstellungen wiederherstellen	<ul style="list-style-type: none">• Daten, Einstellungen und Treiber bleiben erhalten• minimalistisches Betriebssystem	<ul style="list-style-type: none">• 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
<ul style="list-style-type: none">• “bare metal” - neue Hardware• “refresh” - neues OS• “replace” - Upgrade	<ul style="list-style-type: none">• Manuell durch Benutzer• Windows Update durch Benutzer• WSUS durch Benutzer/Admin• Teil-/ Vollautomatisiertes durch Benutzer / Admin	<ul style="list-style-type: none">• Standalone ausgeführt• Innerhalb einer Task-Sequenz

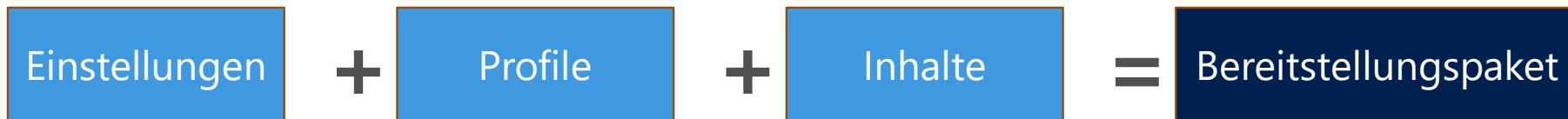
Provisioning Packages

Was ist ein Bereitstellungspaket im Detail?

Format der Bereitstellungspakete ist *.PPKG (WIM Container)

Inhalt von Bereitstellungspaketen:

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



Provisioning Packages

Editions upgrades

- 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 | 29
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.



Papierkorb



sepagoChangeEdition

Windows aktivieren

Wechseln Sie zu den Einstellungen, um
Windows zu aktivieren.



Ich bin Cortana. Frag mich etwas.



10:25
13.04.2016

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

Provisioning: New Features

Added in ADK 1511:

- Run scripts and executables: specify command line, include content

New features in ADK 1607:

- New “simple” provisioning package wizards for common scenarios
- Existing functionality considered “advanced mode”
- Imaging features are deprecated and will be removed in the next release
- The focus is on “just enough configuration” to get the PC to a managed state
- Shared PC mode

Provisioning: Preinstalled software

Preinstalled software on new PCs is still challenging

- No automated way to remove it
- Need to remove “trialware” while leaving hardware configuration apps
- Considering options for a future Windows 10 feature update

Many customers will consider this a deal-breaker

- Scripting is possible to remove undesired stuff, but this is a maintenance headache (different software on different PCs)
- Ask OEMs to provide “clean” images without this (some may charge extra for this)
- Surface devices are a good example, no extra software is ever included

Working on provisioning processes to remove them, but could be time-consuming (e.g. PC reset)

Provisioning: Preinstalled software

Windows-Designer für die Imageerstellung und -konfiguration

Datei | Bereitstellen | Startseite Project_1

Schritte

- Gerät einrichten
- Netzwerk einrichten
- Bei Active Directory registrieren
- Finish

Gerätename

Geben Sie einen eindeutigen Gerätenamen mit 15 Zeichen ein. Falls Sie Unterstützung beim Generieren eines eindeutigen Namens benötigen:
%SERIAL% umfasst eine hardwarespezifische Seriennummer, und %RANDx% generiert zufällige Zeichen der Länge x.

Beispielwerte für Gerätenamen:

- Contoso-%SERIAL%
- Fabrikam-%RAND:5%

Contoso-%SERIAL%

Product Key

Optional: Geben Sie einen Product Key ein, um Windows zu aktualisieren.

XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX

Zum erweiterten Editor wechseln

Weitere Informationen

Weiter

Version: 10.0.14393.0

Projekt: Einfache Bereitstellung Edition: All Windows desktop editions

Provisioning: Changing the SKU

Moving from Pro to Enterprise has gotten consistently easier

- Windows 7: Wipe and load
- Windows 8.1: In-Place Upgrade
- Windows 10 1507: Provisioning package, MDM policy, plus a reboot
- Windows 10 1607: Change product key, no reboot

Multiple options for doing it:

- Use SLMGR.vbs to change key
- Use a provisioning package
- Using an MDM policy

Only supported at this point for Pro to Enterprise (no other SKUs)

Provisioning: Forward looking

Azure AD Join

- No way to automate, even in Windows 10 1607
- Planning to address with the next Windows 10 Creators Update
- Likely to be driven by provisioning packages

Integrating provisioning packages into existing processes

- Today, there is no simple way to automate the installation of a provisioning package (e.g. add to a task sequence)
- Looking at PowerShell-driven mechanisms to enable this

Wrap Up Provisioning Packages

Mit Bereitstellungspaketen können Sie...

Endbenutzern über USB, FTP, E-Mail ein Konfigurationspaket zukommen lassen

zur Laufzeit Geräte von Endbenutzern (Notebooks, Desktops, Smartphones) konfigurieren

mit Hilfe von DISM, Konfigurationen innerhalb ihres Images aufnehmen

Für Bereitstellungspakete...

benötigen Sie lokale Administratorenrechte

benötigen Sie manuelle Interaktion (keine Kommandozeile). Eine „Installation“ über eine SW-Management Lösung ist nicht möglich.

gibt es kein „wirkliches“ Rollback

wird Crapware / Bloatware nicht immer berücksichtigt

Microsoft IT Camps – Windows 10 Enterprise Deployment

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:

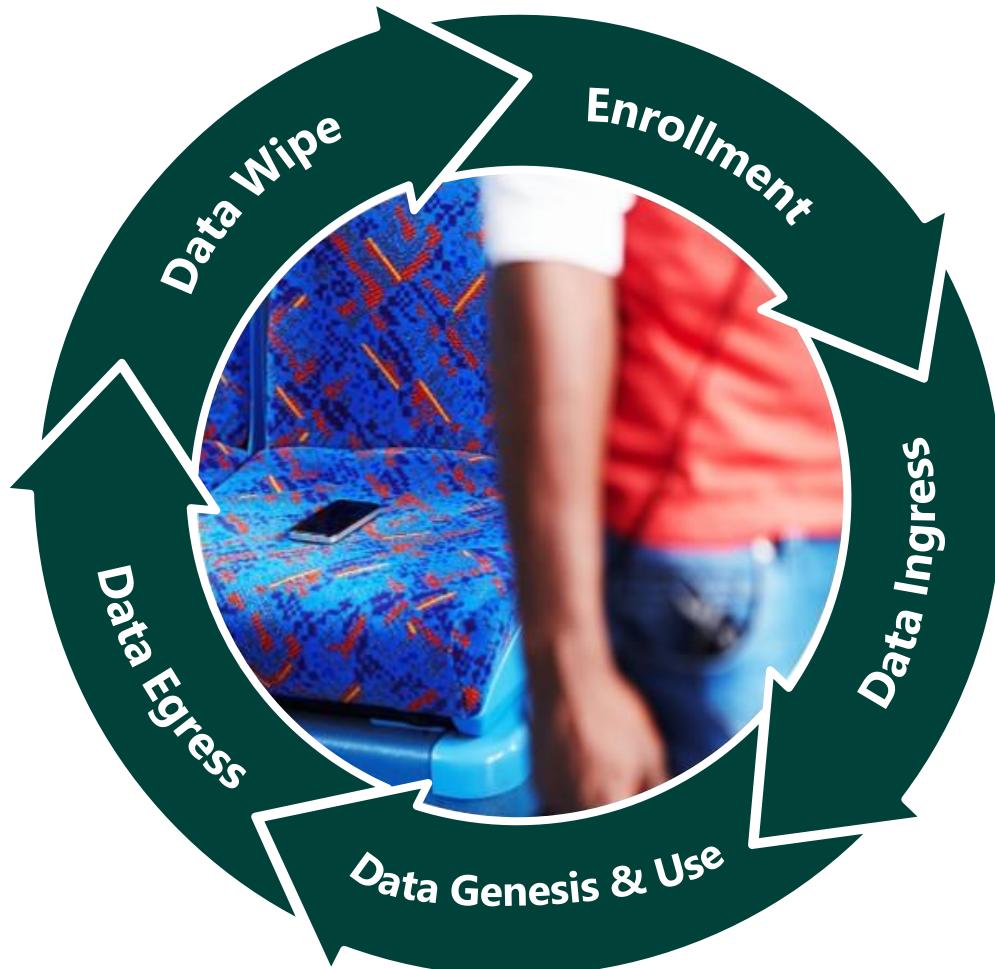
- Administrator defines a set of enterprise approved applications that are allowed to access data
- Network Boundaries are defined (IP ranges, Cloud locations e.g. O365) - Defines if data is coming from or going to a defined "Enterprise" location

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

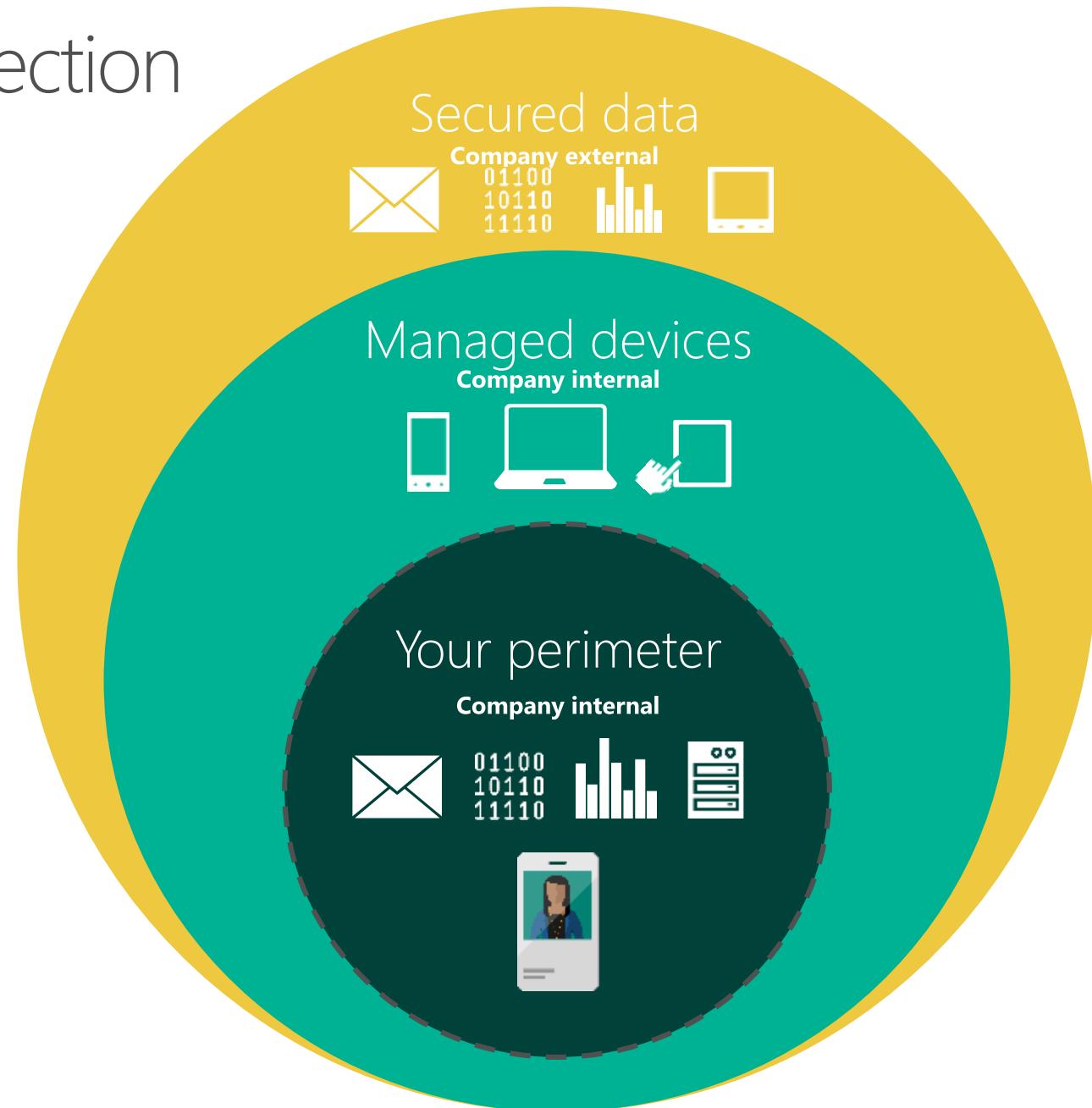
Data Leak & Data Sharing Protection

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?

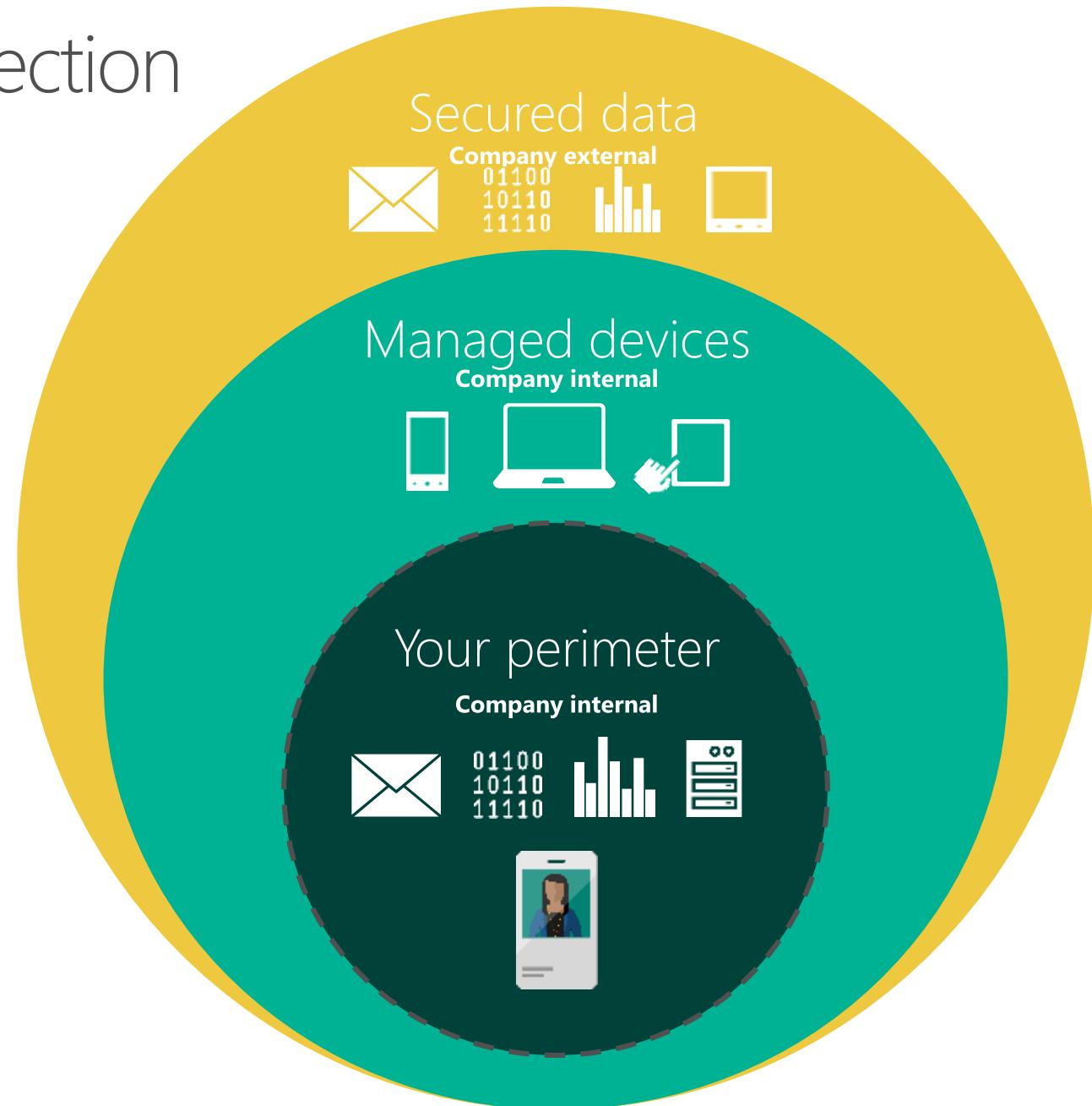
Keep all data on premises?!?

Managing all identities
in your own directory?!?

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

Accept that data will leak?!?

Or

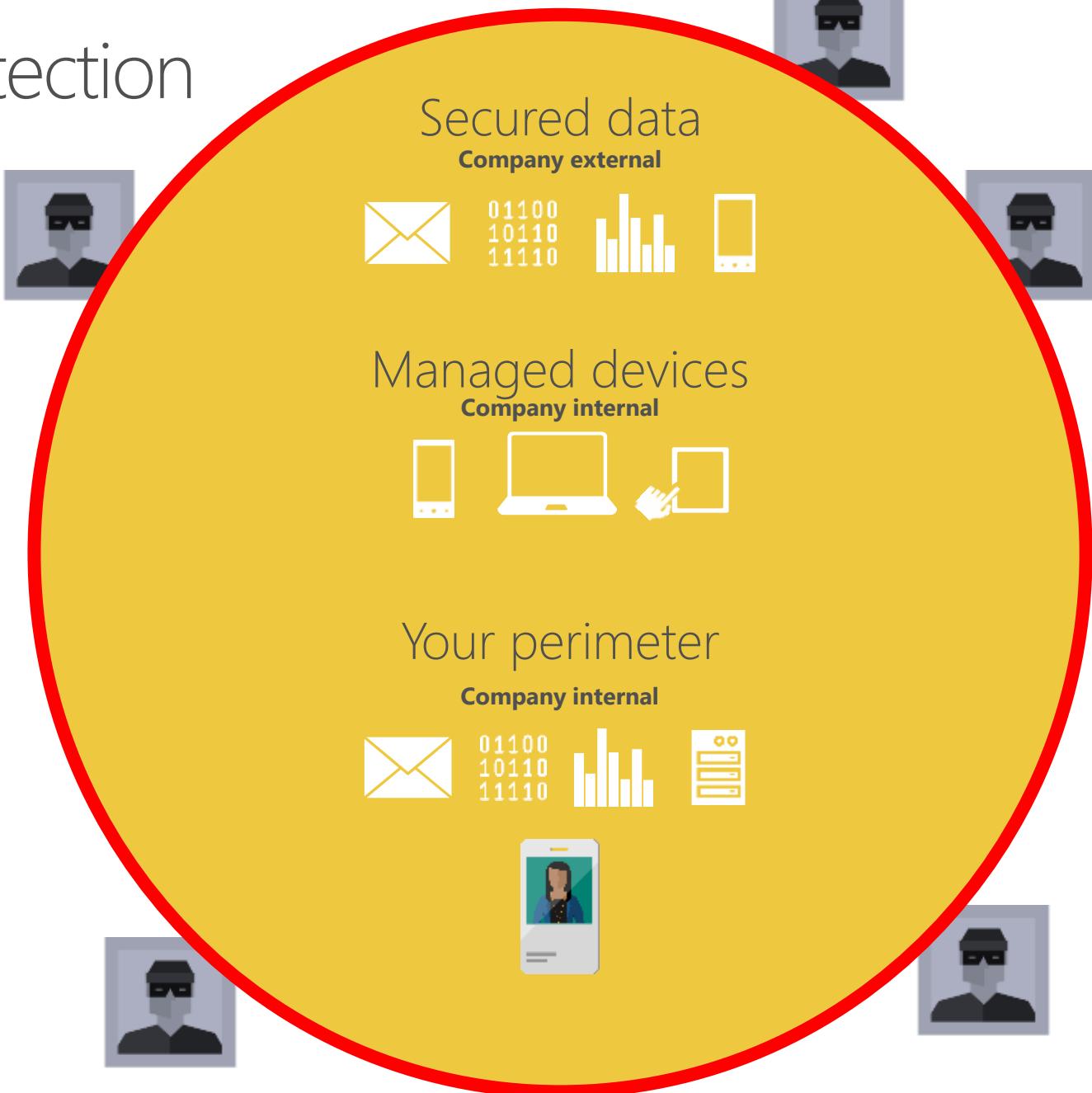


Data Leak & Data Sharing Protection

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

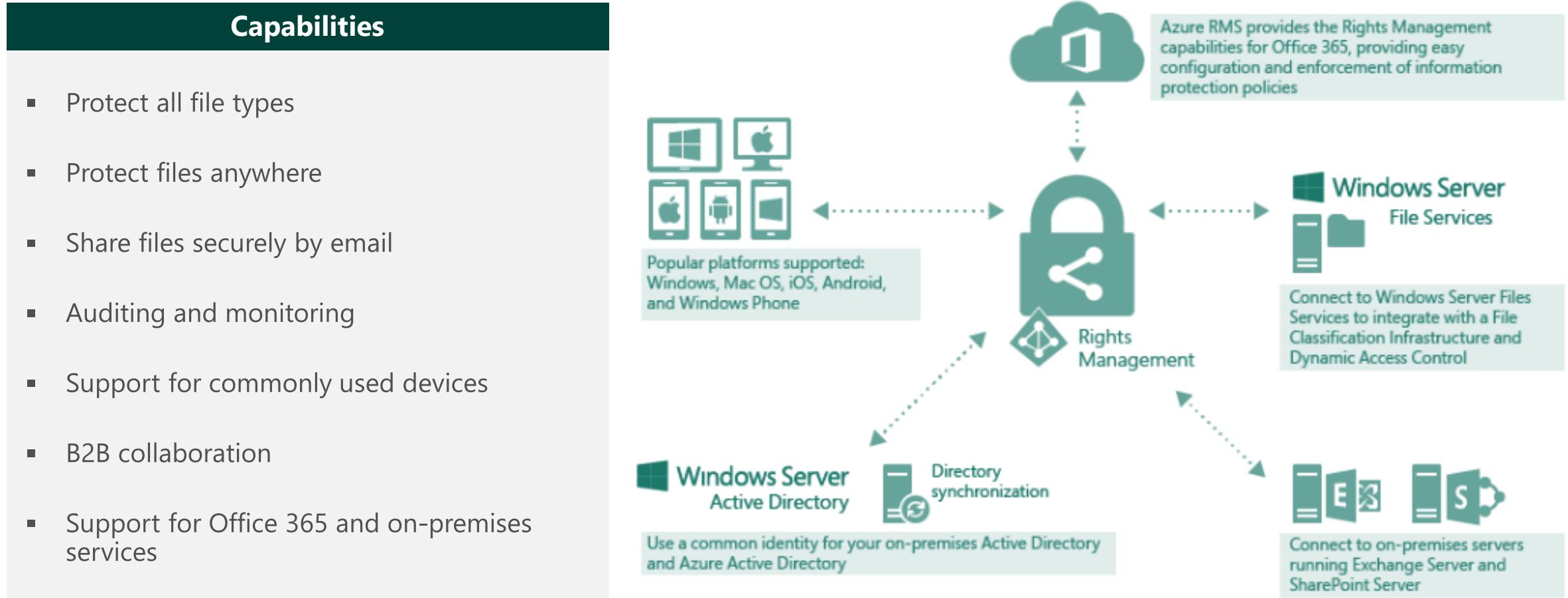
- Classify, label and protect data at the time of creation or modification
- Persistent protection that travels with your data
- Enable safe sharing with customers and partners
- Simple, intuitive controls help users make the right decisions and stay productive
- Visibility and control over shared data
- Deployment and management flexibility

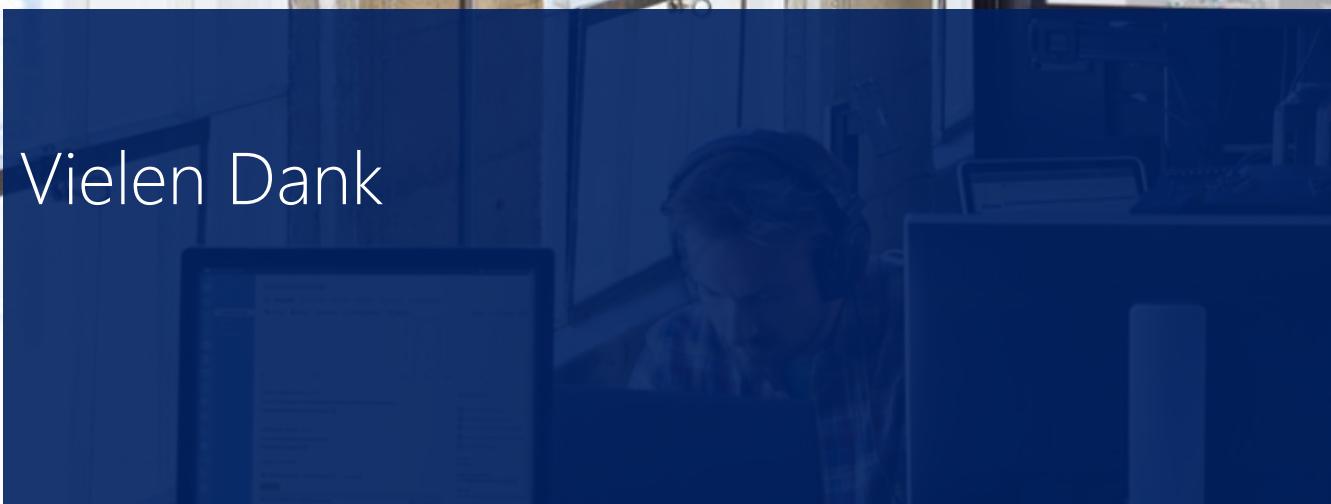
Requirements

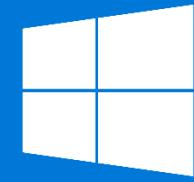
- Azure Subscription that includes Azure Rights Management Services
- Global Administrator rights to activate the Rights Management service
- Windows 7 SP1 device or above, with Office 2010 and above

Data Leak & Data Sharing Protection

Azure Rights Management Services







Windows 10