Co se změnilo ve Windows 10 z pohledu IT administrátora

Kamil Roman

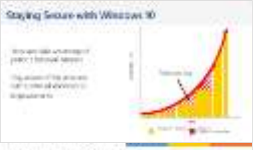
MCSE: Mobility | MCSE: Cloud Platform and Infrastructure | MCSA | MCITP | MCT

konzultace@KamilRT.net

@KamilRT

Agenda

1. Windows as a Service
2. Security
3. Management
4. Deployment
5. What else?
6. Follow-up sessions



Staying Secure with Windows 10

Management Choices

Deployment Choices

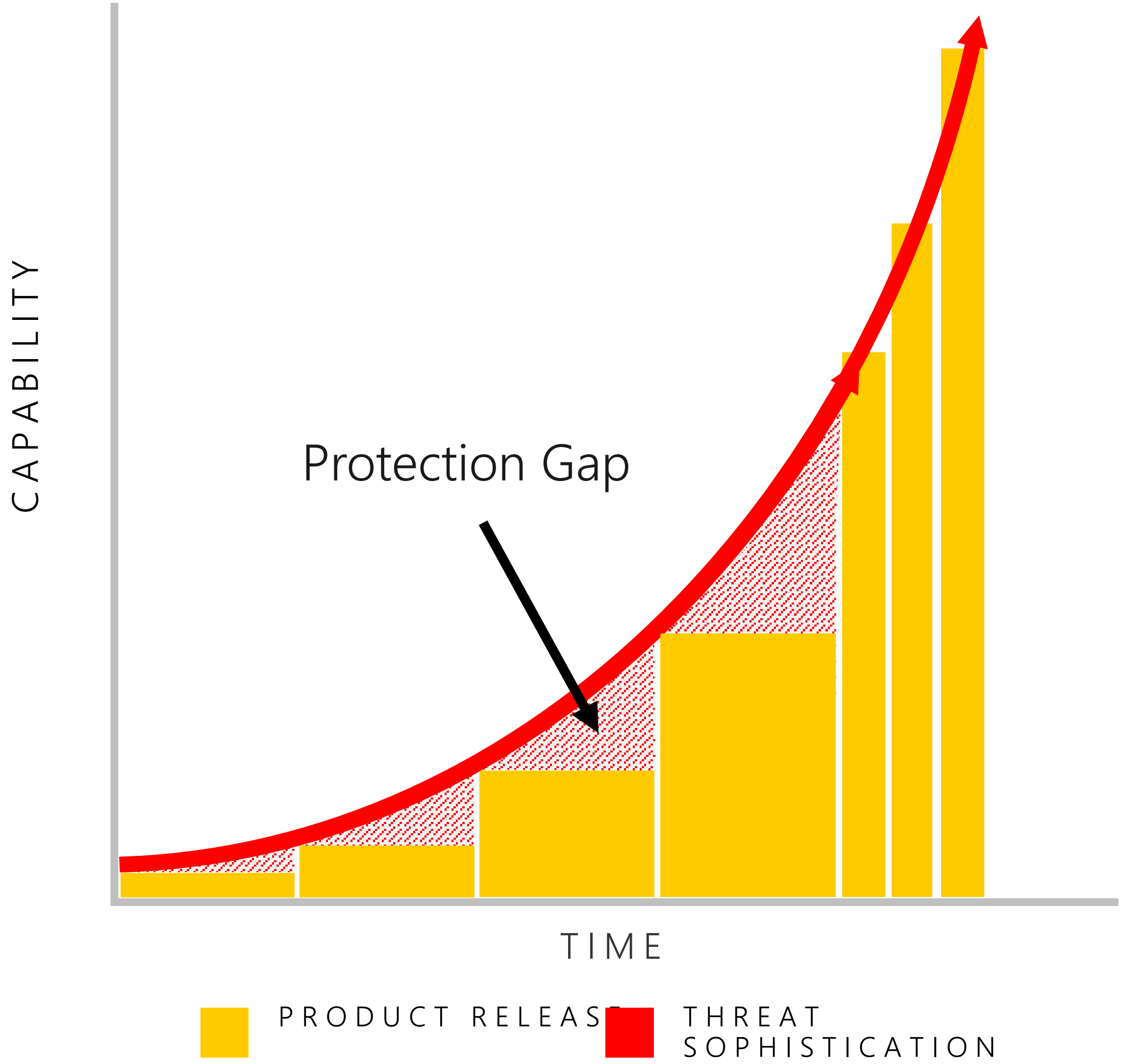
What else?

Follow-up sessions

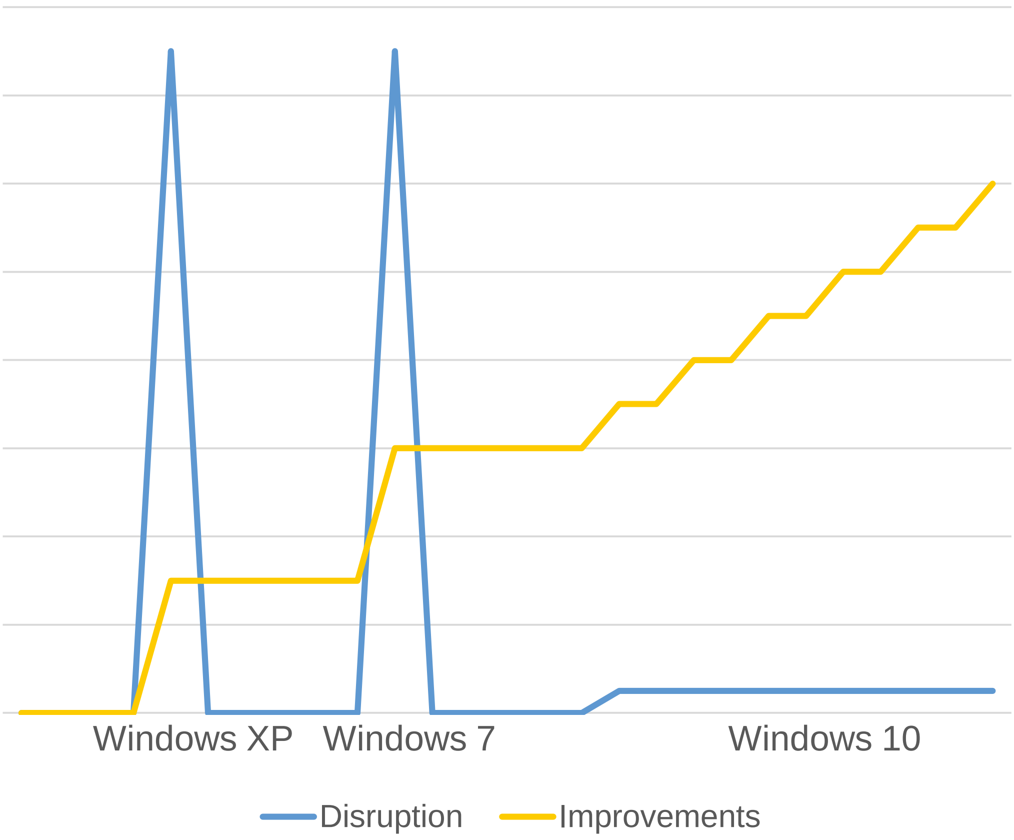
Staying Secure with Windows 10

Attackers take advantage of periods between releases

Stay ahead of the attackers with continual Windows 10 improvements



Improving Productivity with Windows 10

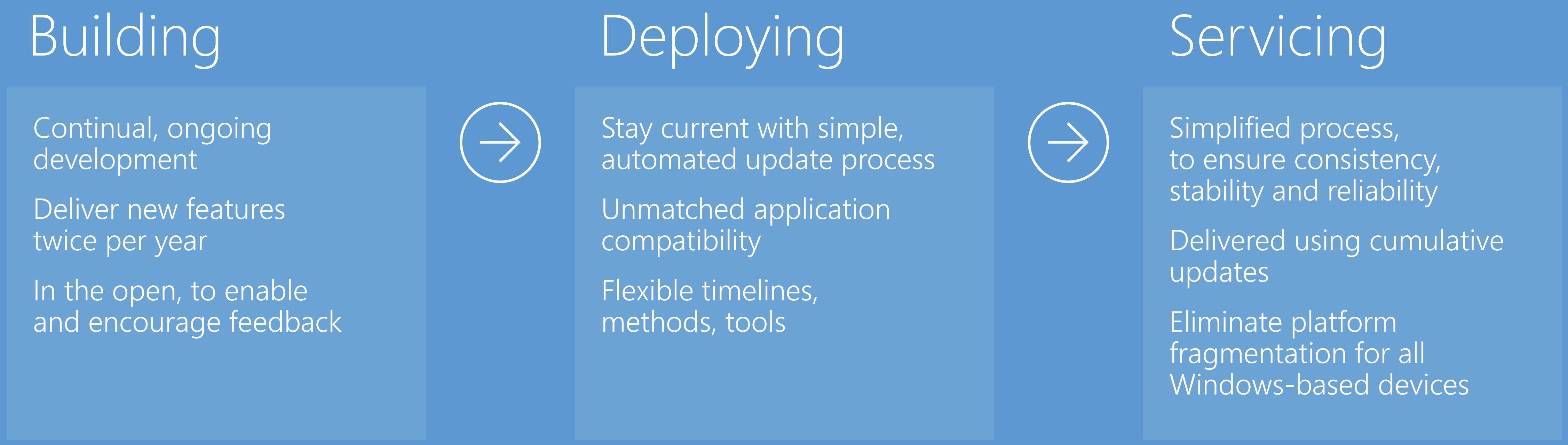


Continual improvements: New features twice per year, adding value and improving productivity

Minimized end-user disruption by having less change with each release

Windows as a Service

A 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

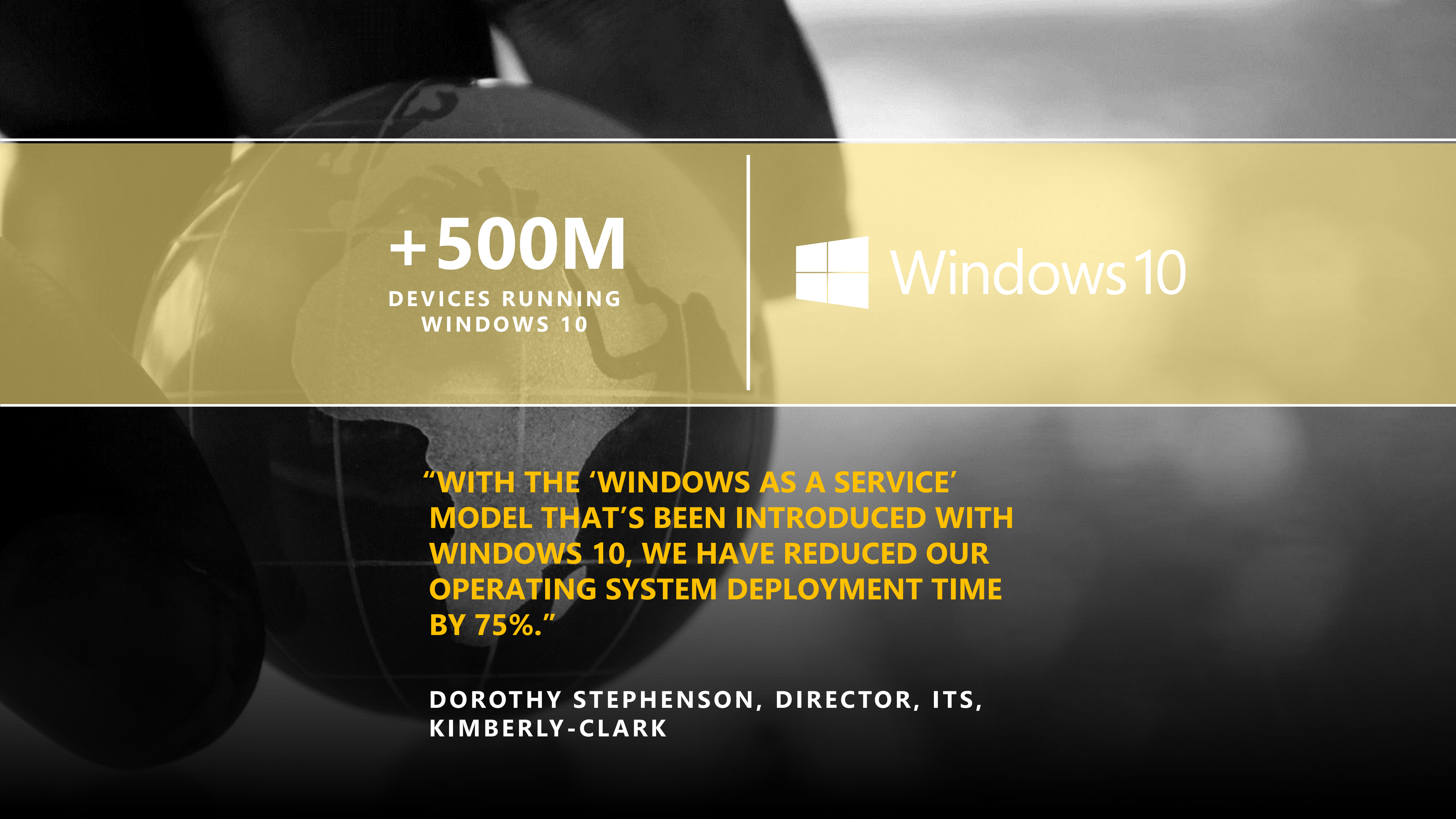
Flexible timelines, methods, tools

Servicing

Simplified process, to ensure consistency, stability and reliability

Delivered using cumulative updates

Eliminate platform fragmentation for all Windows-based devices



+500M

DEVICES RUNNING WINDOWS 10

Windows 10

> “WITH THE ‘WINDOWS AS A SERVICE’ MODEL THAT’S BEEN INTRODUCED WITH WINDOWS 10, WE HAVE REDUCED OUR OPERATING SYSTEM DEPLOYMENT TIME BY 75%.”

DOROTHY STEPHENSON, DIRECTOR, ITS,
KIMBERLY-CLARK

Improving Windows as a Service

Continuing improvements to address customer feedback

Current Challenges	Announced Changes
Windows 10 releases are unpredictable “Two to three times per year” (with exceptions) Release timeframes are not disclosed in advance	Windows 10 releases are predictable Twice every year, targeting March and September
Windows 10 servicing timelines are unclear “We service two CBB releases at all times, with a 60-day grace period” Customers are unable to predict end of servicing dates	Windows 10 servicing timelines are clear Each Windows 10 feature release will be serviced and supported for 18 months from the date of release
Windows 10 updates are too large Periodic feature updates and monthly quality updates are challenging to deploy due to their size	Windows 10 updates are measurably smaller Improvements available in Windows 10 1607 and Windows 10 1703, with further improvements coming later this year (as previously announced)

Aligning Windows 10 and Office 365 ProPlus

Making it easier to stay current with both in lockstep

Current Challenges	Announced Changes
Release schedules are not aligned Windows 10 release schedule is variable Office 365 ProPlus releases every four months	**Release schedules are aligned** Windows 10 and Office 365 ProPlus will release twice per year, targeting March and September
Servicing timelines are different Windows 10 releases are serviced and supported for at least 18 months Office 365 ProPlus releases are serviced and supported for 12 months	**Servicing timelines are identical** Windows 10 and Office 365 ProPlus will be serviced and supported for 18 months from the date of release

Windows as a Service Supplemental Support

Desktop operating systems	Date of availability	End of support*
Windows 7 SP1	February 22, 2011	January 14, 2020
Windows 10 version 1507	July 29, 2015	May 9, 2017
Windows 10 version 1511	November 10, 2015	~~October 10,2017~~ April 2018**
Windows 10 version 1607	August 2, 2016	Tentatively March 2018
Windows 10 version 1703	April 5, 2017	Tentatively September 2018
Windows 10 version 1709	November 9, 2017	Tentatively May 2018

* Microsoft may extend End of support at it’s discretion.

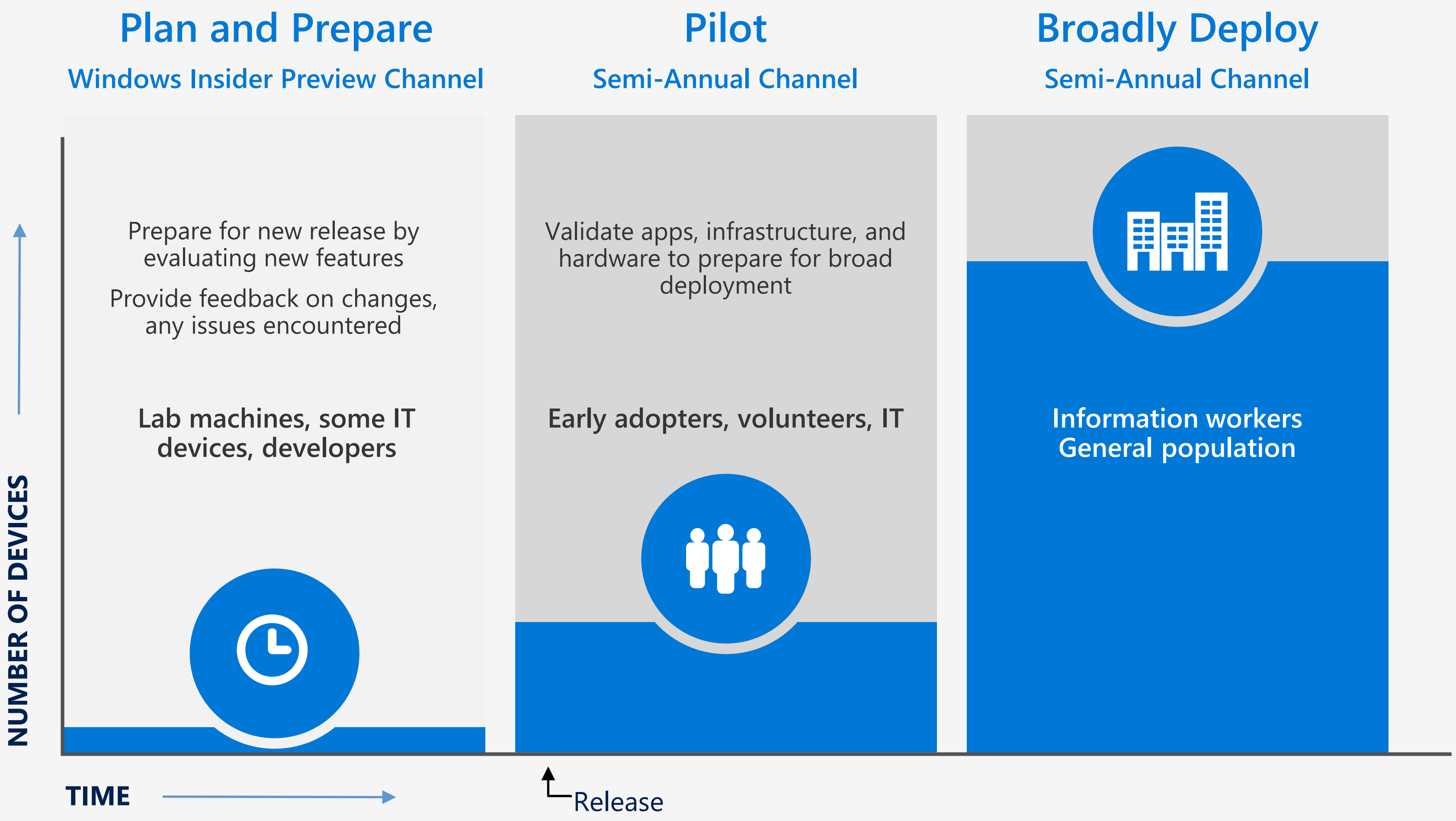
** On November 20, 2017 Microsoft announced a 6-month extension for 1511.

Aligning Terminology

	Monthly Channel Monthly 1 month of support	Semi-Annual Channel 2x / year 18 months of support	Long Term Servicing Channel Every 2-3 years 10 years of support (5+5)
Office	✓	✓	
Windows		✓	✓

Windows as a service

Moving from project to process



Plan and Prepare

Windows Insider Preview Channel

Prepare for new release by evaluating new features

Provide feedback on changes, any issues encountered

Lab machines, some IT devices, developers

Pilot

Semi-Annual Channel

Validate apps, infrastructure, and hardware to prepare for broad deployment

Early adopters, volunteers, IT

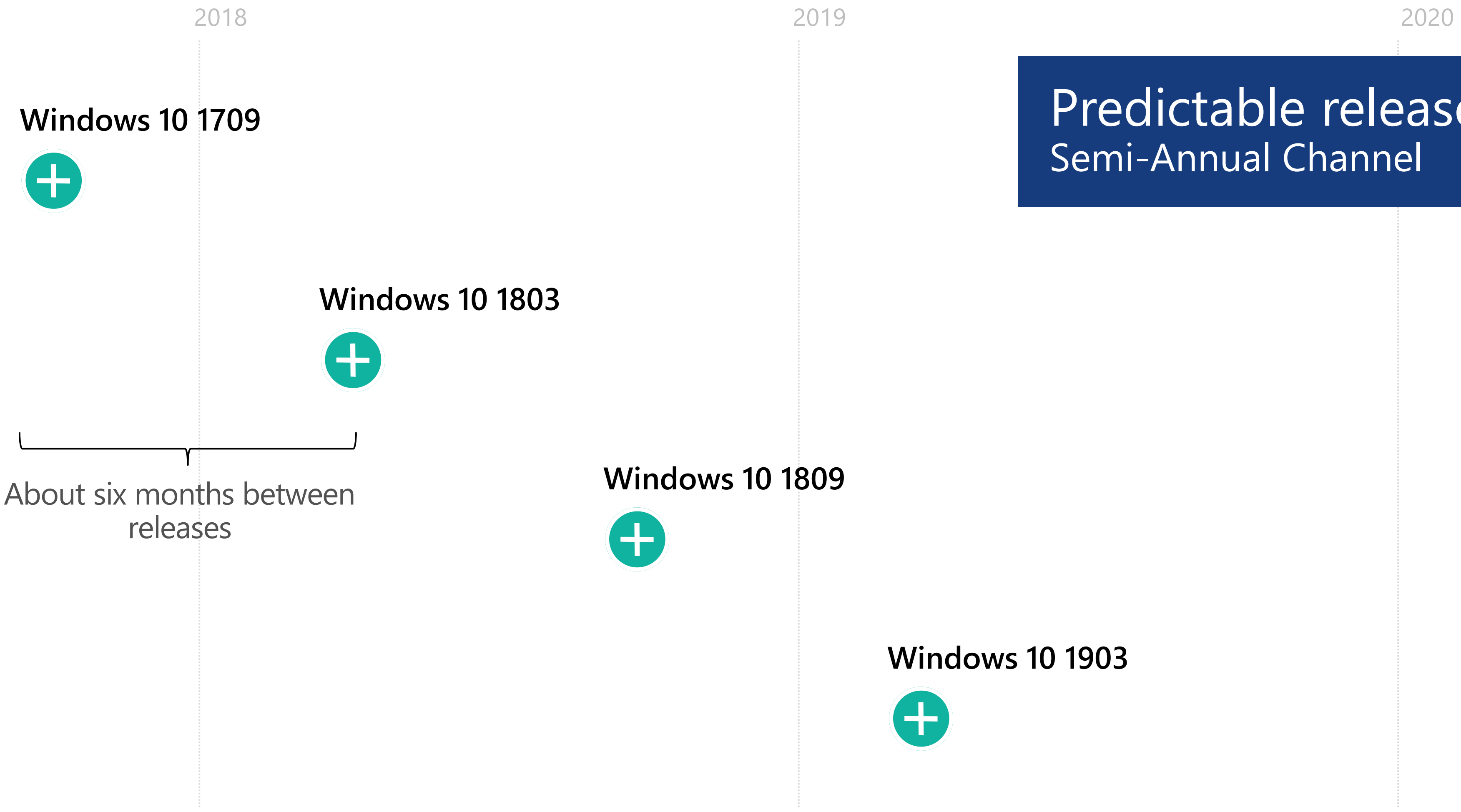
Broadly Deploy

Semi-Annual Channel

Information workers
General population

Staying Current

Key things to know about Windows as a Service



2018

2019

2020

Windows 10 1709

Windows 10 1803

About six months between releases

Windows 10 1809

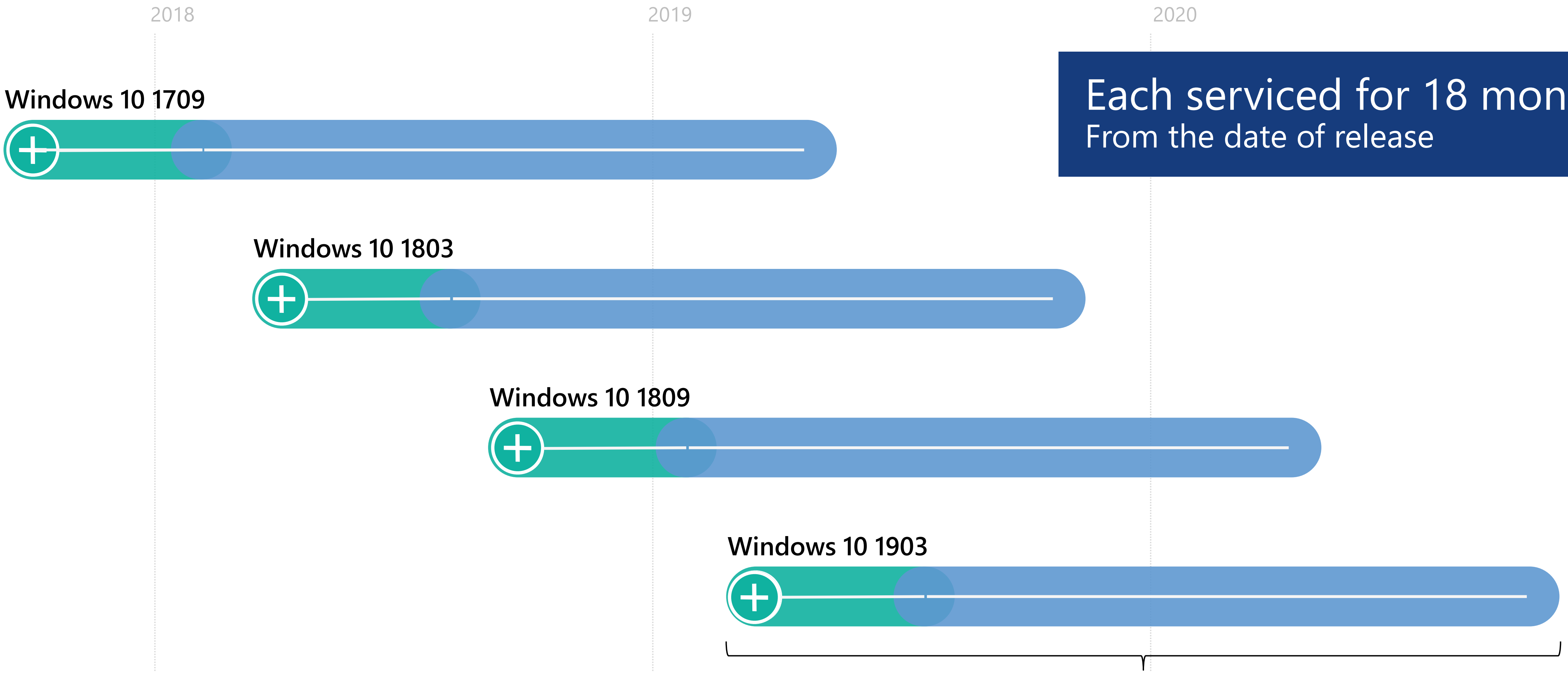
Windows 10 1903

Predictable releases, twice per year

Semi-Annual Channel

Staying Current

Key things to know about Windows as a Service

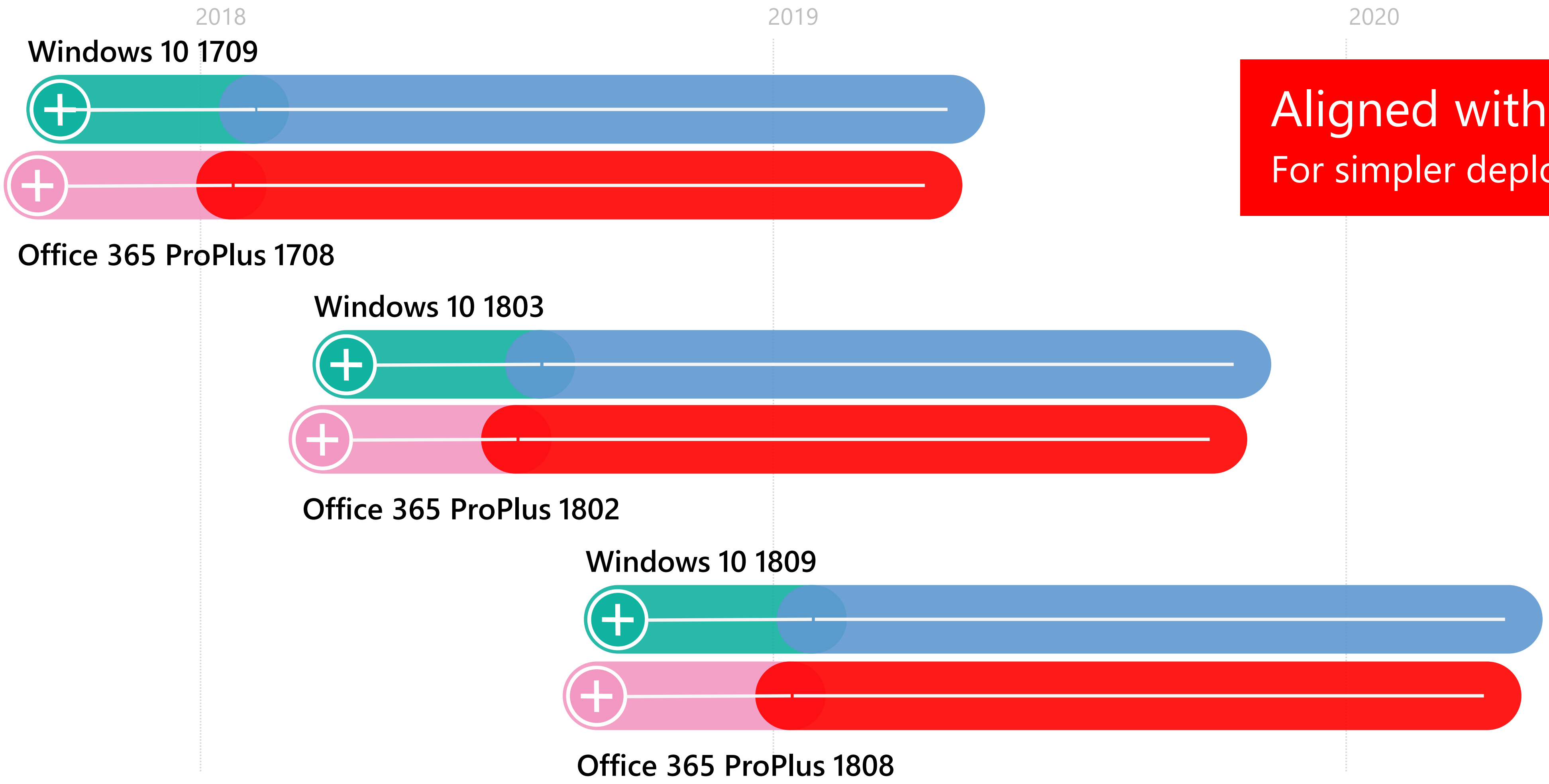


Each serviced for 18 months
From the date of release

18 months for each release

Staying Current

Key things to know about Windows as a Service

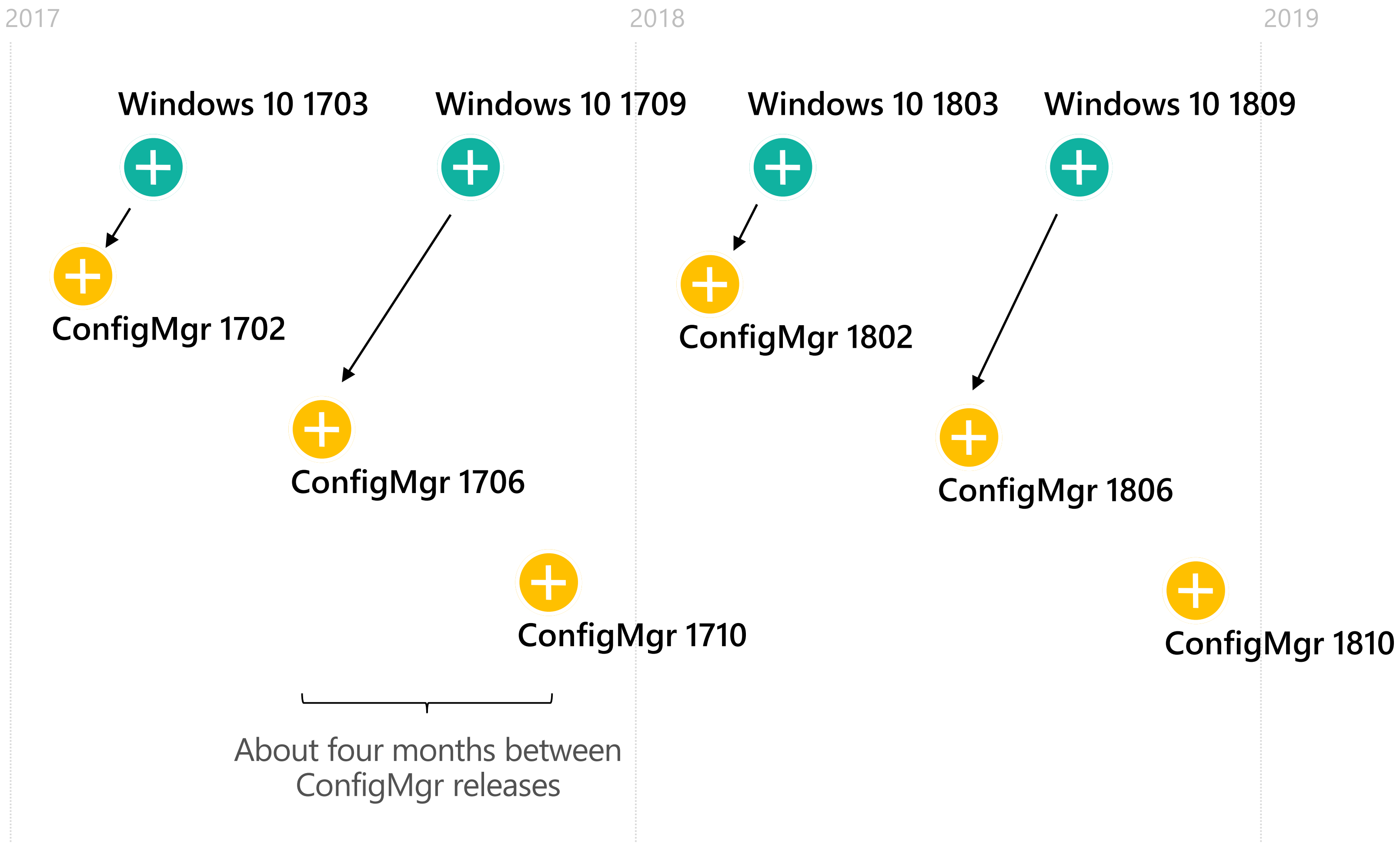


Aligned with Office

For simpler deployment planning

Staying Current

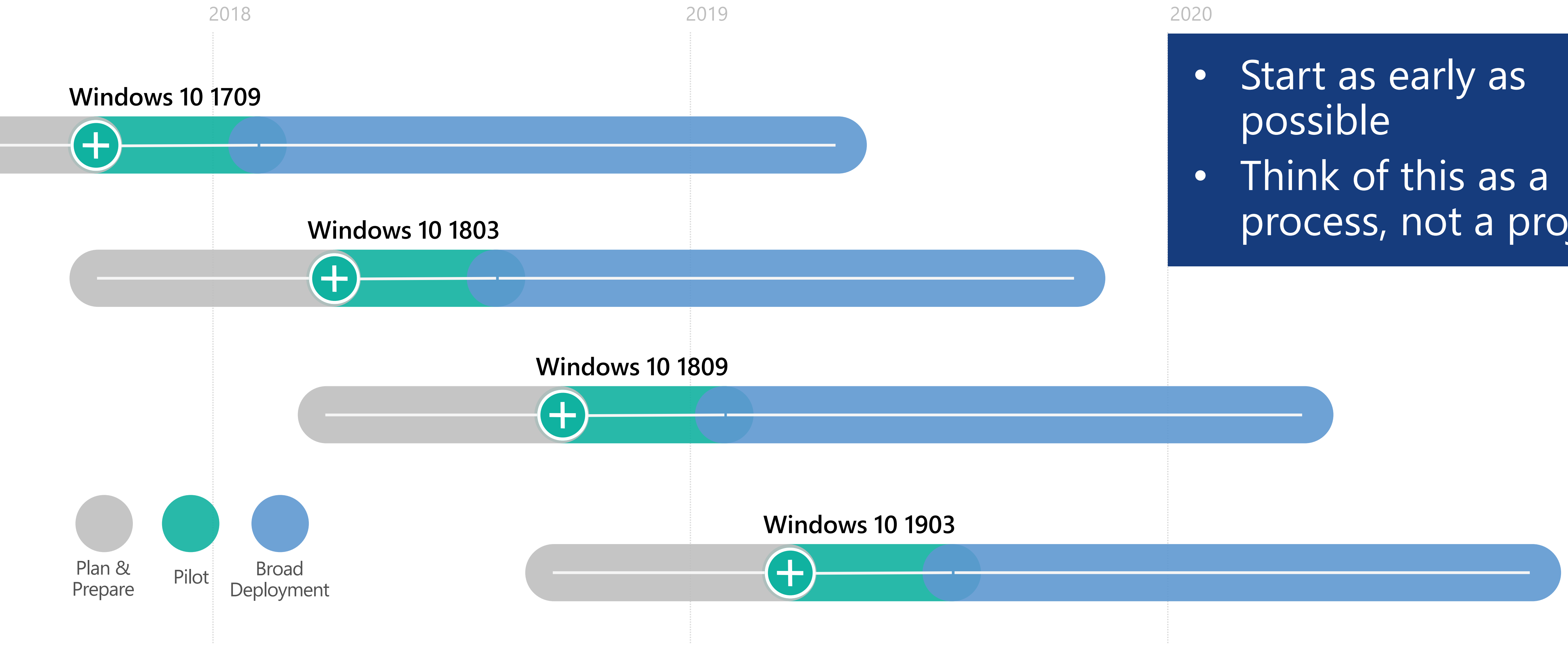
Key things to know about Windows as a Service



Supported by ConfigMgr Current Branch

Staying Current

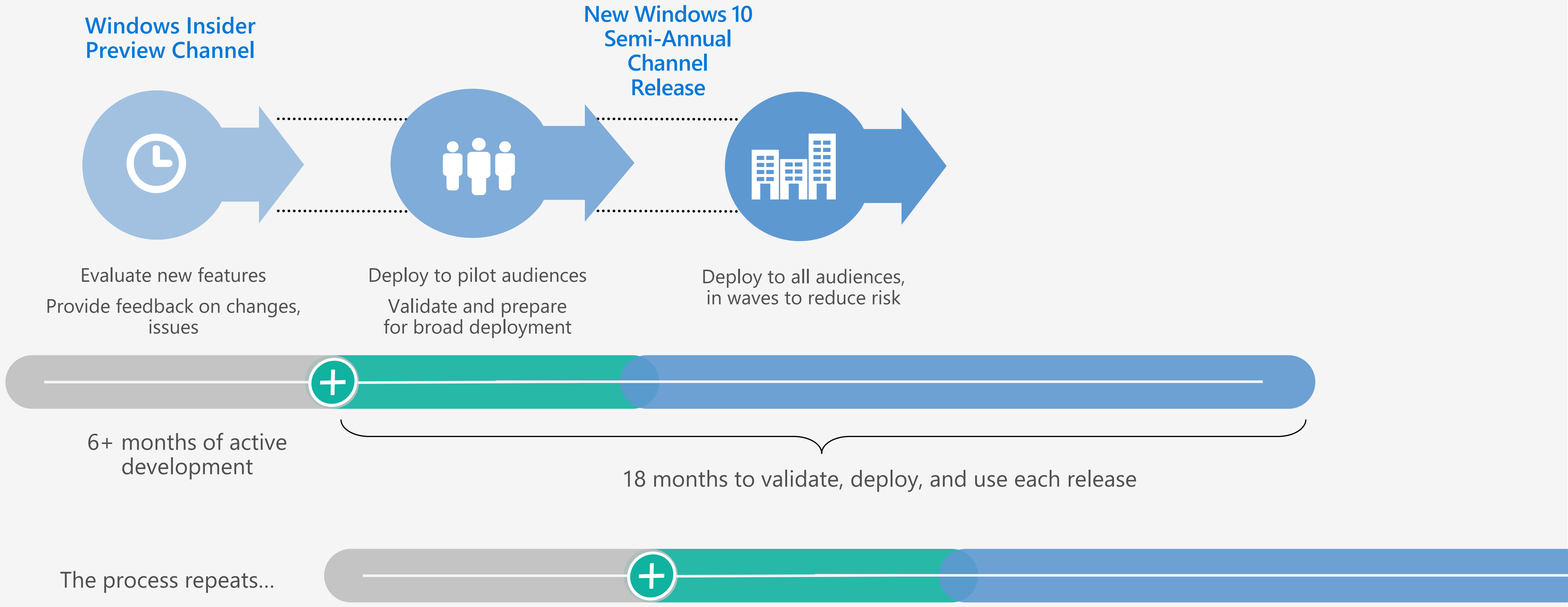
Key things to know about Windows as a Service



- Start as early as possible
- Think of this as a process, not a project

Windows as a service

The process of a release



Windows Insider Preview Channel

New Windows 10 Semi-Annual Channel Release

Evaluate new features

Provide feedback on changes, issues

Deploy to pilot audiences

Validate and prepare for broad deployment

Deploy to all audiences, in waves to reduce risk

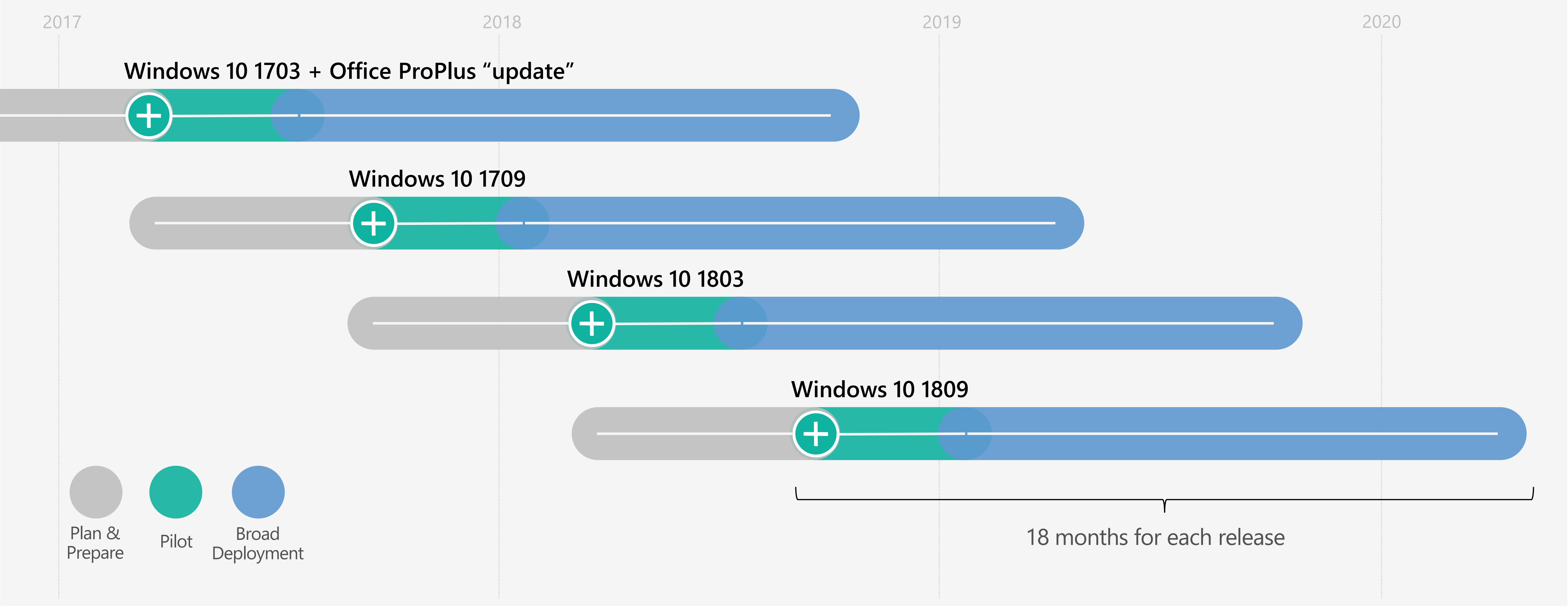
6+ months of active development

18 months to validate, deploy, and use each release

The process repeats…

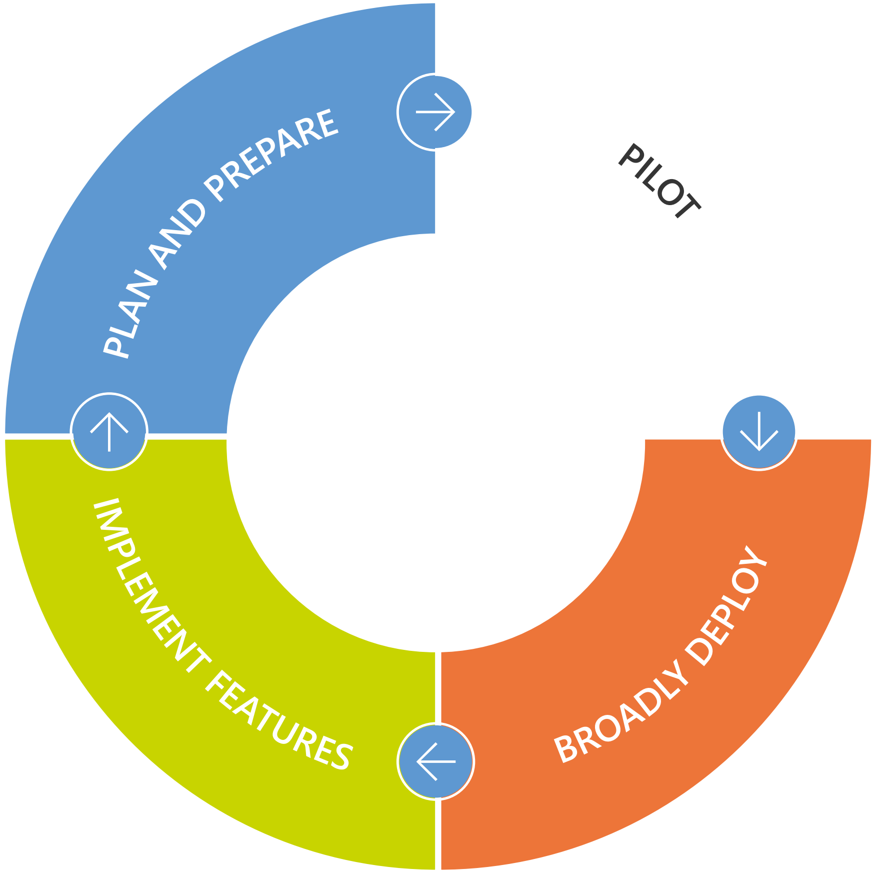
Windows as a Service

Predictable and clear timeframes



What needs to change

Creating teams responsible for implementing the process



🟦 Plan and Prepare Team

- Working with Insider Preview builds
- Providing feedback on features and compatibility
- Identifying needed feature implementation teams

🟧 Deployment Team

- Performing business-critical app validation
- Conducting initial pilots for each release
- Driving broad deployments of each release
- Reacting to issues encountered

🟩 Feature Implementation Teams

- Formed as needed to implement new features
- Can be done synchronously with the deployment of a release or later

How to validate apps

Minimize the up-front effort, focus on reactive approach

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

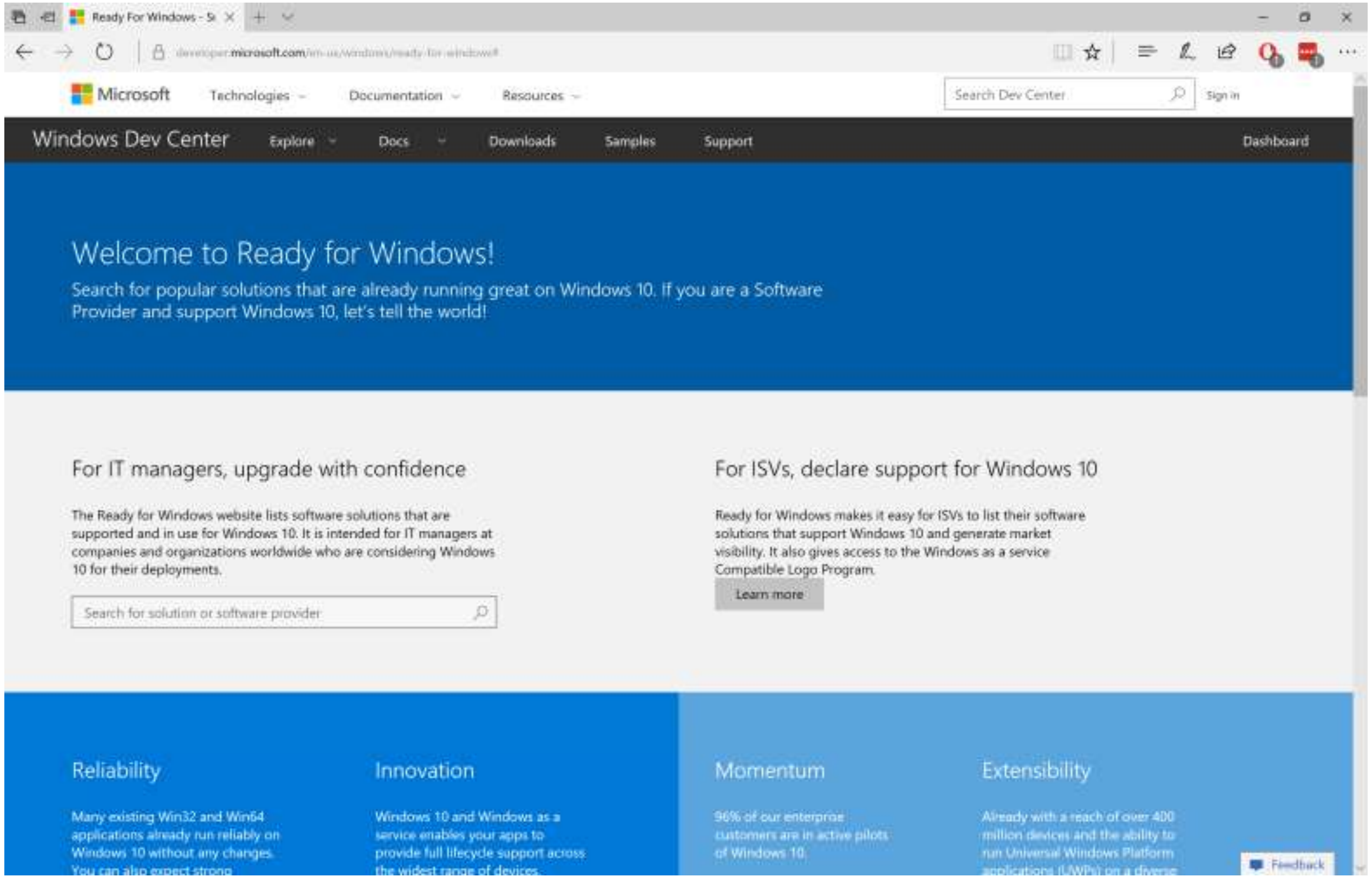
- Structured testing, using predefined test plans executed with business and IT experts
- Automated if possible
- Target small percentage of apps

→

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

Compatibility in Windows 10



Welcome to Ready for Windows!

Search for popular solutions that are already running great on Windows 10. If you are a Software Provider and support Windows 10, let's tell the world!

For IT managers, upgrade with confidence

The Ready for Windows website lists software solutions that are supported and in use for Windows 10. It is intended for IT managers at companies and organizations worldwide who are considering Windows 10 for their deployments.

For ISVs, declare support for Windows 10

Ready for Windows makes it easy for ISVs to list their software solutions that support Windows 10 and generate market visibility. It also gives access to the Windows as a service Compatible Logo Program.

Reliability

Many existing Win32 and Win64 applications already run reliably on Windows 10 without any changes. You can also expect strong

Innovation

Windows 10 and Windows as a service enables your apps to provide full lifecycle support across the widest range of devices.

Momentum

96% of our enterprise customers are in active pilots of Windows 10.

Extensibility

Already with a reach of over 400 million devices and the ability to run Universal Windows Platform applications (UWPs) on a diverse

Get links to Windows 10 ISV support statements

Get usage information for every app version, and use that to target testing

http://www.readyforwindows.com

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

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 (CYOD) ▪ Bring Your Own Device (BYOD)

Active Directory

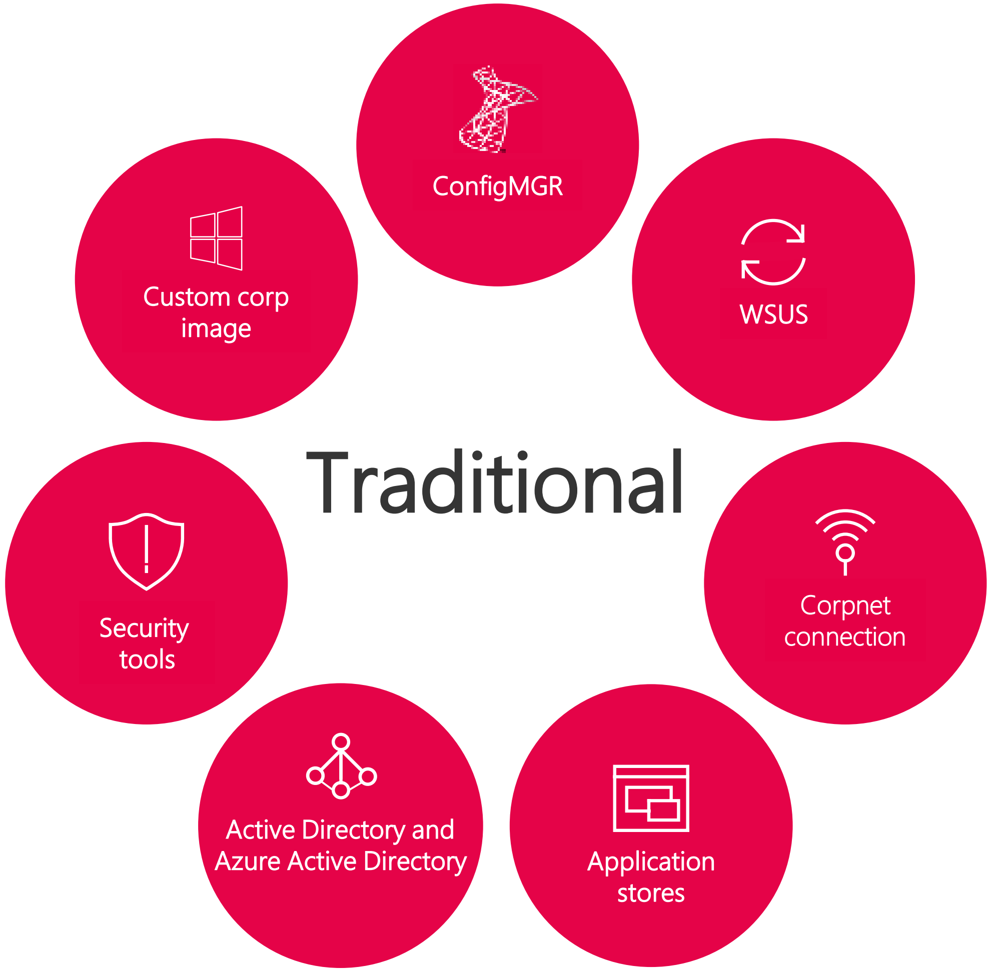
Management

- Existing supported versions are fully supported for Windows 10

- New Group Policy templates are needed to support the new settings available for current release of Windows 10
  - ➢ Administrative Templates (.admx) for Windows 10 Fall Creators Update: *https://www.microsoft.com/en-us/download/details.aspx?id=56121*

- No new Active Directory schema updates or specific functional levels are currently required for core Windows 10 product functionality, although subsequent upgrades could require these to support new features

Revolution



Traditional

ConfigMGR

WSUS

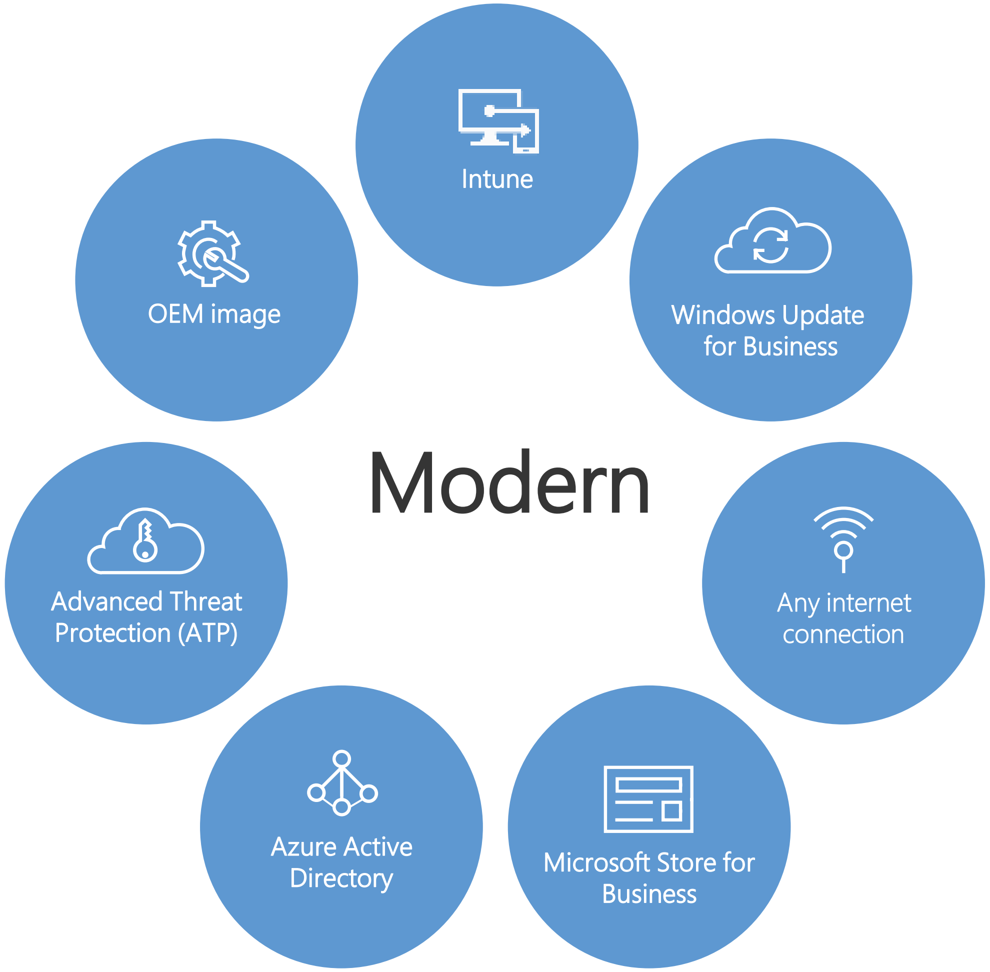
Corpnet connection

Application stores

Active Directory and Azure Active Directory

Security tools

Custom corp image



Modern

Intune

Windows Update for Business

Any internet connection

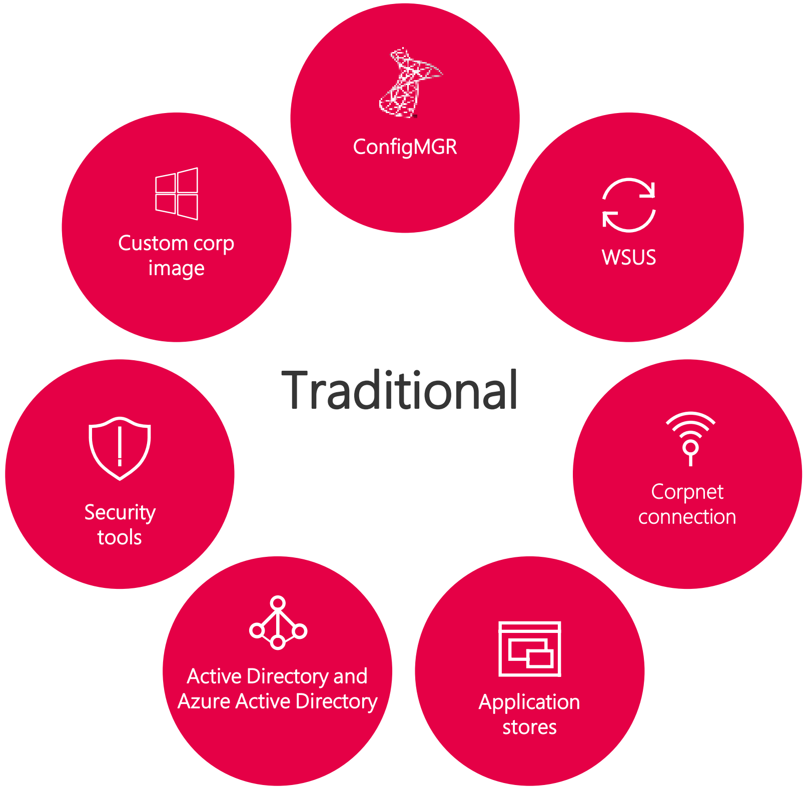
Microsoft Store for Business

Azure Active Directory

Advanced Threat Protection (ATP)

OEM image

Evolution



Traditional

ConfigMGR

Custom corp image

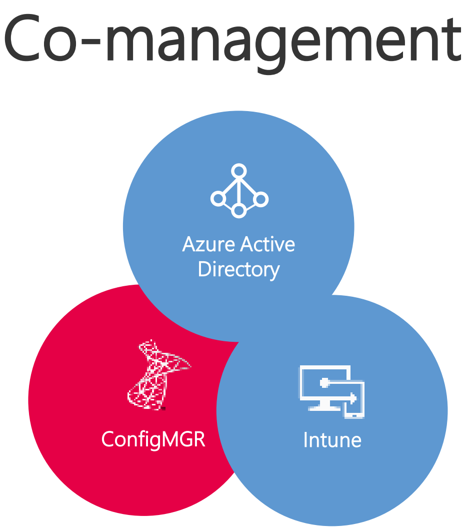
WSUS

Security tools

Corpnet connection

Active Directory and Azure Active Directory

Application stores



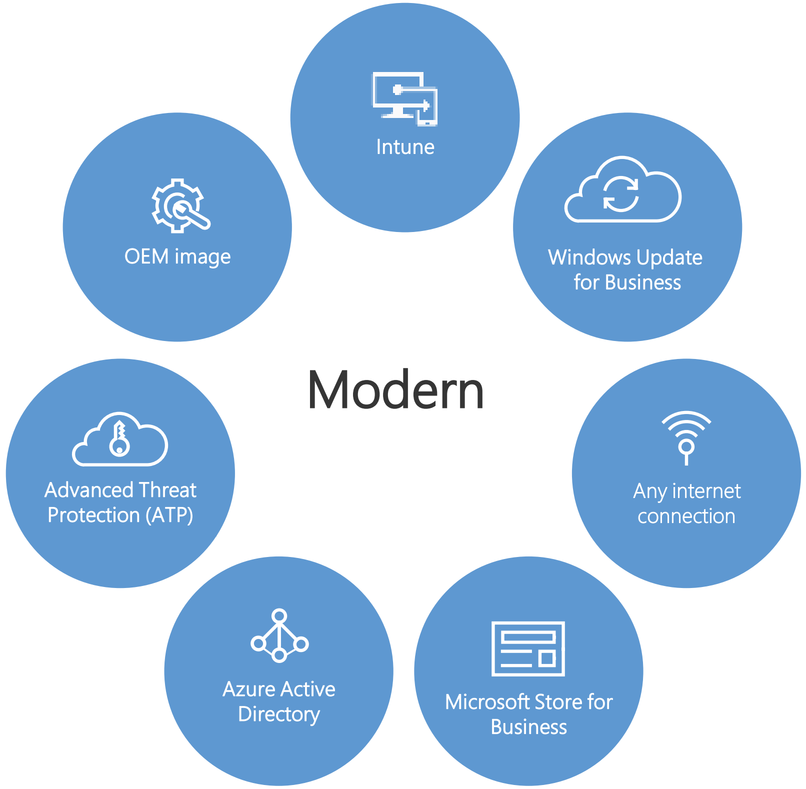
Co-management

Azure Active Directory

ConfigMGR

Intune

- Allows organizations to take a first step toward Modern Management to build confidence and momentum
- Intune is primary management solution
- ConfigMGR is available as contingency



Modern

Intune

OEM image

Windows Update for Business

Advanced Threat Protection (ATP)

Any internet connection

Azure Active Directory

Microsoft Store for Business

Evolution

	Traditional →	Co-Management →	Modern
Connectivity	Corpnet connection	**Any internet connection**	Any internet connection
Operating system image	Custom corp image	**OEM image**	OEM image
Identity	Active Directory and Azure Active Directory	**Azure Active Directory**	Azure Active Directory
Device management	System Center Configuration Manager (ConfigMGR)	ConfigMGR + **Intune**	**Intune**
Updates	Windows Server Update Services (WSUS)	WSUS + **WUfB**	**Windows Update for Business (WUfB**)
Security	Security tools	Security tools	Security tools
Applications	Multiple app stores	Multiple app stores	**Microsoft Store for Business (MSfB)**

New in 1709 – Co-Management

Prerequisites

- Technical Preview for Configuration Manager version 1709
- Azure AD
- EMS or Intune license for all users
- Intune subscription (MDM authority in Intune set to **Intune**)

Note - Hybrid MDM environment (Intune integrated with Configuration Manager), cannot enable co-management.

Additional prerequisites for existing Configuration Manager clients

- Windows 10, version 1709 (Fall Creators Update) and later
- Hybrid Azure AD joined (joined to AD and Azure AD)

Additional prerequisites for new Windows 10 devices

- Windows 10, version 1709 (Fall Creators Update) and later
- Cloud Management Gateway in Configuration Manager

Migratable Workloads

Compliance policies

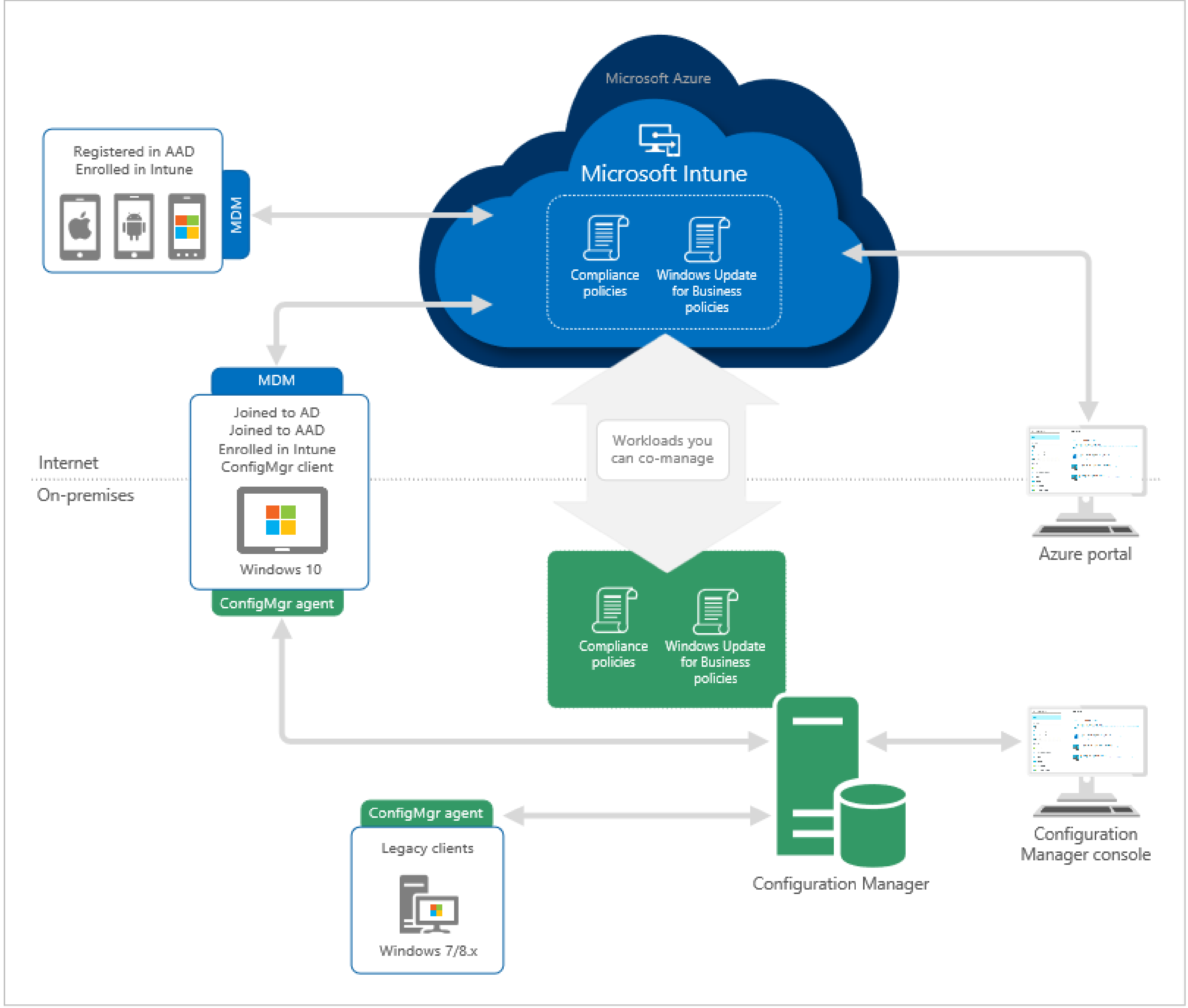
- Compliance policies define the rules and settings that a device must comply with to be considered compliant by conditional access polices. You can also use compliance policies to monitor and remediate compliance issues with devices independently of conditional access.

Windows Update for Business policies

- Windows Update for Business policies let you configure deferral policies for Windows 10 feature updates or quality updates.

https://docs.microsoft.com/en-us/sccm/core/get-started/capabilities-in-technical-preview-1709#co-management-for-windows-10-devices

Co-Management Architectural Overview



Deployment Choices

Wipe & Load

Familiar enterprise process for all scenarios

1. Capture Data / Settings
2. Deploy (custom) OS image
3. Inject Drivers
4. Install Apps
5. Restore Data / Settings

Still an option for all scenarios

In-Place Upgrade

Let Windows do the work

1. Preserve data, settings, apps, drivers
2. Install (standard) OS image
3. Restore everything

Recommended for existing Windows 7 / 8 / 8.1 devices

Recommended to upgrade Windows 10 devices to Creators update

Provisioning/AutoPilot

New capability for new devices

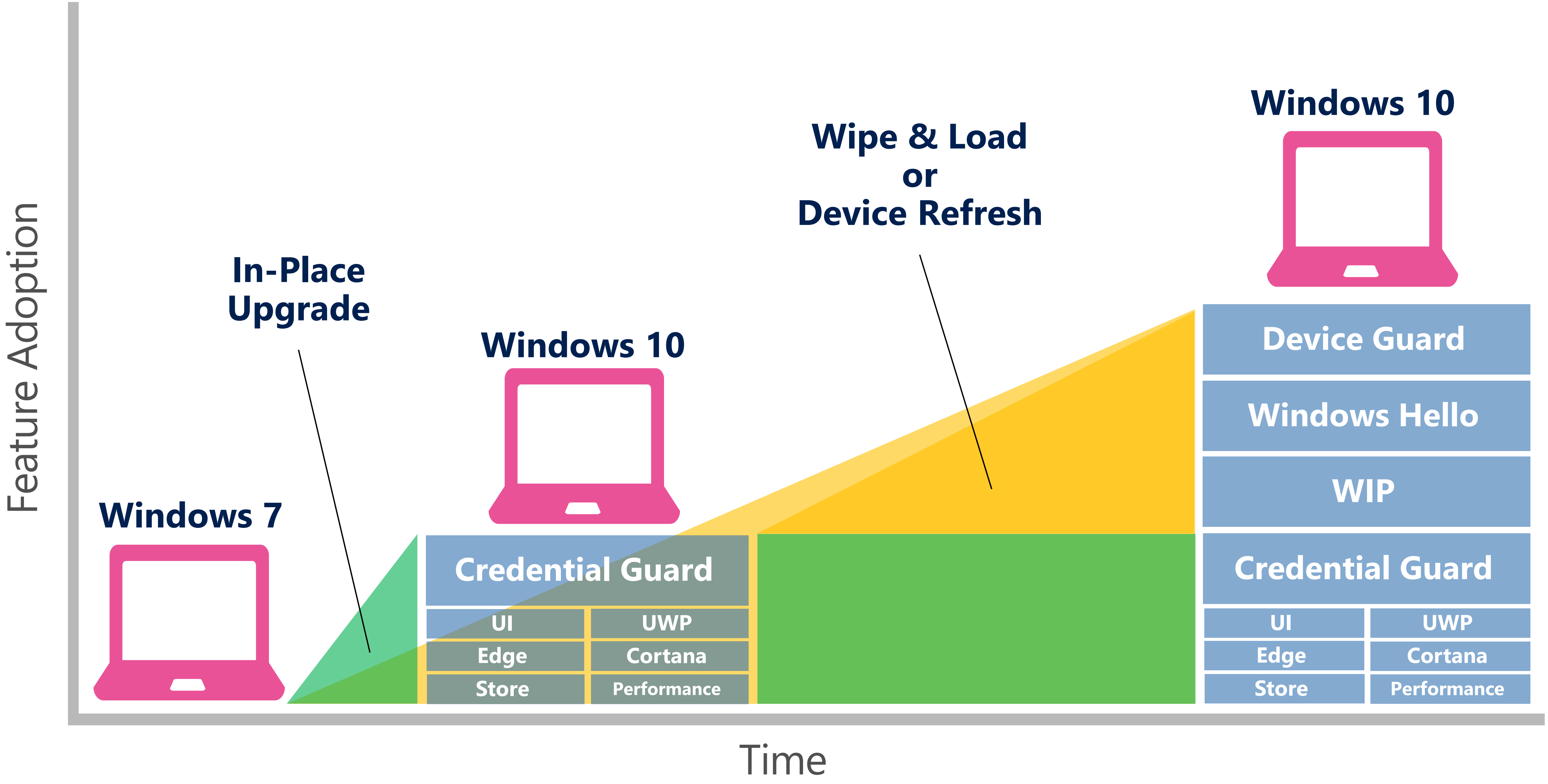
Transform into an enterprise device

- Remove bloatware and 3rd party branding
- Add organizational apps
- Add organizational configuration

For Windows 10 CYOD scenarios

Management feature

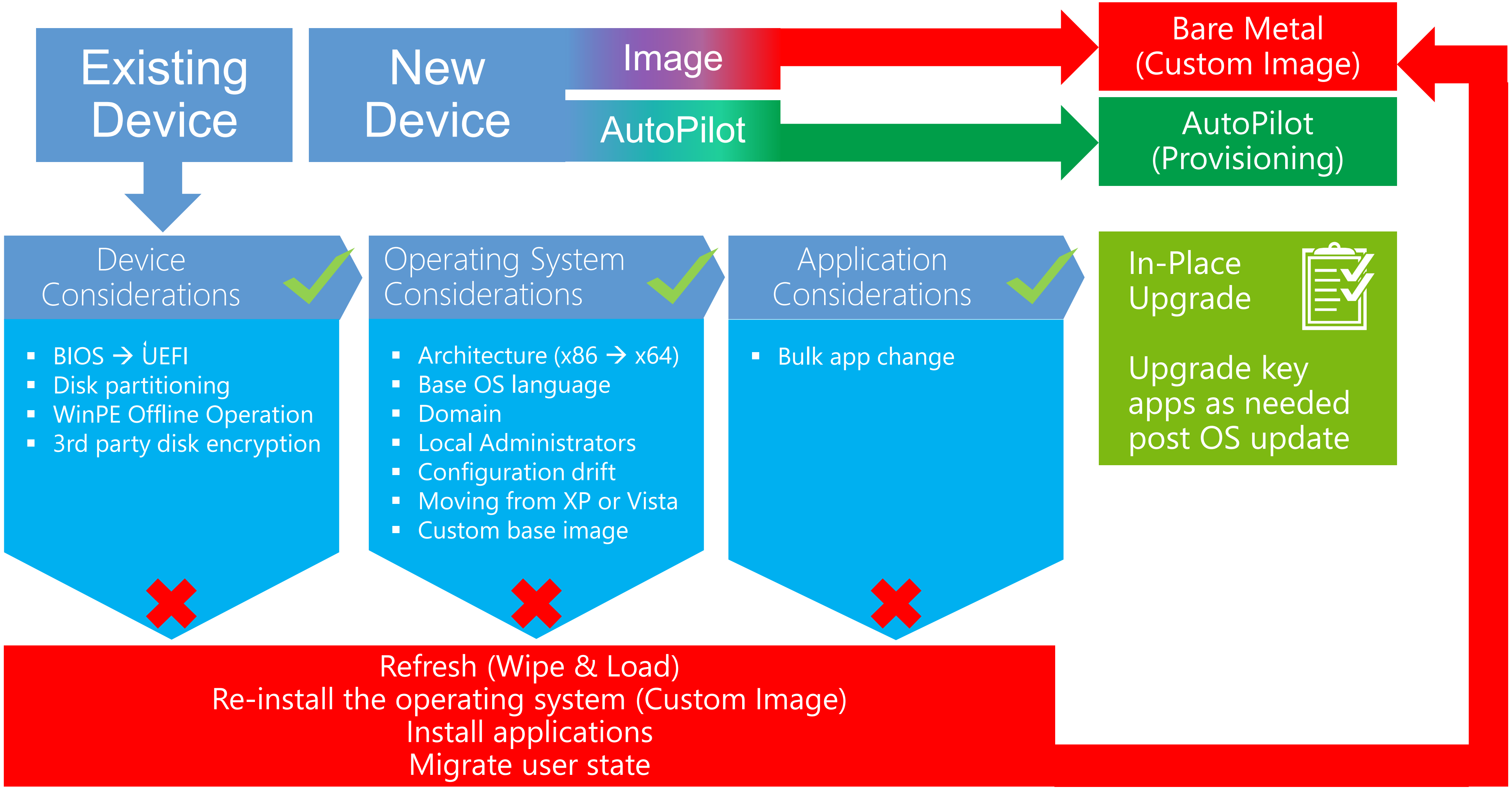
Transformation Choices



Transformation Effort

	Refresh	Replace	Upgrade
Pre-Reqs	▪ Assessing systems requires time ▪ Extent of assessment depends on approach ▪ Upgrade required infrastructure to support Windows 10		
Engineer	▪ Image must be designed/model specific ▪ Finalized when compatibility information is known	▪ Image must be designed ▪ Finalized when compatibility information is known ▪ Remote data migration solution	▪ No image or data migration solution required
Deploy	▪ Image is typically larger than Microsoft media	▪ Image is typically larger than Microsoft media	▪ Smallest media is from Microsoft
Post-Install	▪ All app installers must be compatible with Windows 10 for re-install	▪ All app installers must be compatible with Windows 10 for re-install ▪ User data must be restored from remote repository	▪ Only apps determined to require re-installation must have compatible installers ▪ Compatible/non-blocking apps are migrated
Rollback	▪ No rollback ▪ Re-deploy old OS and re-configure system	▪ Revert to old machine ▪ Data on old system becomes increasing stale	▪ Built-in rollback for 10 days ▪ Data on windows.old system becomes increasing stale
Duration	▪ Fast	▪ Slow	▪ Faster

Deploying Windows 10



Existing Device

New Device

Image

AutoPilot

Bare Metal (Custom Image)

AutoPilot (Provisioning)

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 Assessment and Deployment Kit

- New tools
  - Windows Imaging and Configuration Designer (ICD)

- Updated tools
  - User State Migration Tool (USMT)
- Supports Windows Vista and above as a source OS, Windows 7, and above as a target OS
- New capabilities for creating provisioning packages containing drivers, apps
  - DISM
- New commands to add provisioning packages
- Ability to apply an image as a "Compact OS"
  - Windows PE

RTW version available now

- Moved to the Windows Hardware Dev Center
  https://docs.microsoft.com/en-us/windows-hardware/get-started/adk-install

Compact OS

- Simple deployment option

- Compresses all Windows files to save disk space
- Transparent to the user
- Successor to WIMBoot, with fewer limitations
- Windows updates automatically get compressed too

– Easy to deploy

- Uses standard partition structure, hiding compressed files on the same volume
- **DISM /Apply-Image … /Compact:ON** command line option takes care of the details
- Can be implemented after the fact as well

– Disk space savings

- About **3GB** saved on an x64 system
- Ideal for Windows systems with **32GB** drives or smaller

Reducing the Windows Footprint

New recovery process

- No extra disk space

- Leverages the existing OS files (WINDOWS\WINSXS) to reconstruct the OS
- No separate partition needed

  – Recovery preserves updates

- All but the last 28 days of Windows updates are kept, with new ones discarded just in case those are the reason for the reset
- Recent driver updates will also be discarded
- Language packs will be preserved

Moving from BIOS to UEFI

Challenges

Many UEFI-Capable devices are running Windows in BIOS emulation mode today

- Running older versions of Windows due to application compatibility reasons
- Using CSM or Compatibility Support Module to allow booting in legacy BIOS mode to support some Option ROMs (e.g. Video BIOS, PXE) that don’t support UEFI

Moving existing PCs from BIOS emulation to native UEFI is challenging:

- Use OEM tools to reconfigure firmware
- Move data off, repartition disk
- Apply Windows 10 image
- Move data back

Windows 10 security features require UEFI Firmware

- E.g. Secure Boot, Device Guard, Credential Guard
- Upgrading devices from Windows 7/8.1 in BIOS mode to Windows 10 is not enough

MBR2GPT Tool

Usage

You can use MBR2GPT to perform the following:

- **Within the Windows PE environment (Offline)**:
  Convert any attached MBR-formatted disk to GPT, including the system disk. (*Recommended*)
- **From within the currently running OS (Online)**:
  Convert any attached MBR-formatted disk to GPT, including the system disk.
- **Can be run in validation-only mode**

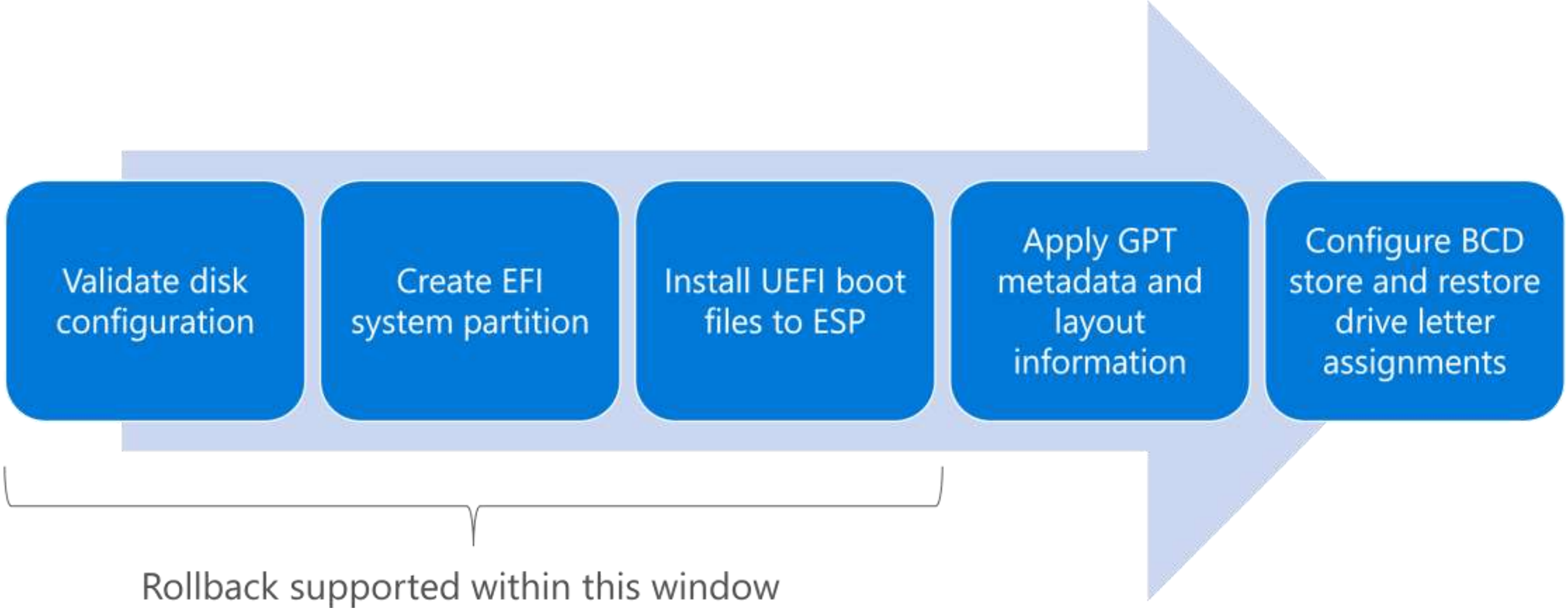
Requirements

- The MBR2GPT tool requires Windows 10 Creators Update
- Can convert earlier version of Windows 10 (e.g. 1507, 1511, 1607) but must use WinPE Boot Image of 1703 in Offline mode
- Earlier version of Windows (e.g. 7, 8, 8.1) must upgrade first to Windows 10 to boot from GPT

BitLocker Consideration

- Protection must be suspended on all BitLocker-encrypted volumes of the disk
- Recreate protectors to re-enable protection

HOW MBR2GPT WORKS



Validate disk configuration

Create EFI system partition

Install UEFI boot files to ESP

Apply GPT metadata and layout information

Configure BCD store and restore drive letter assignments

Rollback supported within this window

HOW HELLO **PROTECTS CREDENTIALS**

Strong authentication via multiple factors

- Uses two factors for authentication (e.g.: PC + PIN or Biometric)
- Asymmetrical Keys (i.e: Private/Public)

User credentials protected by hardware

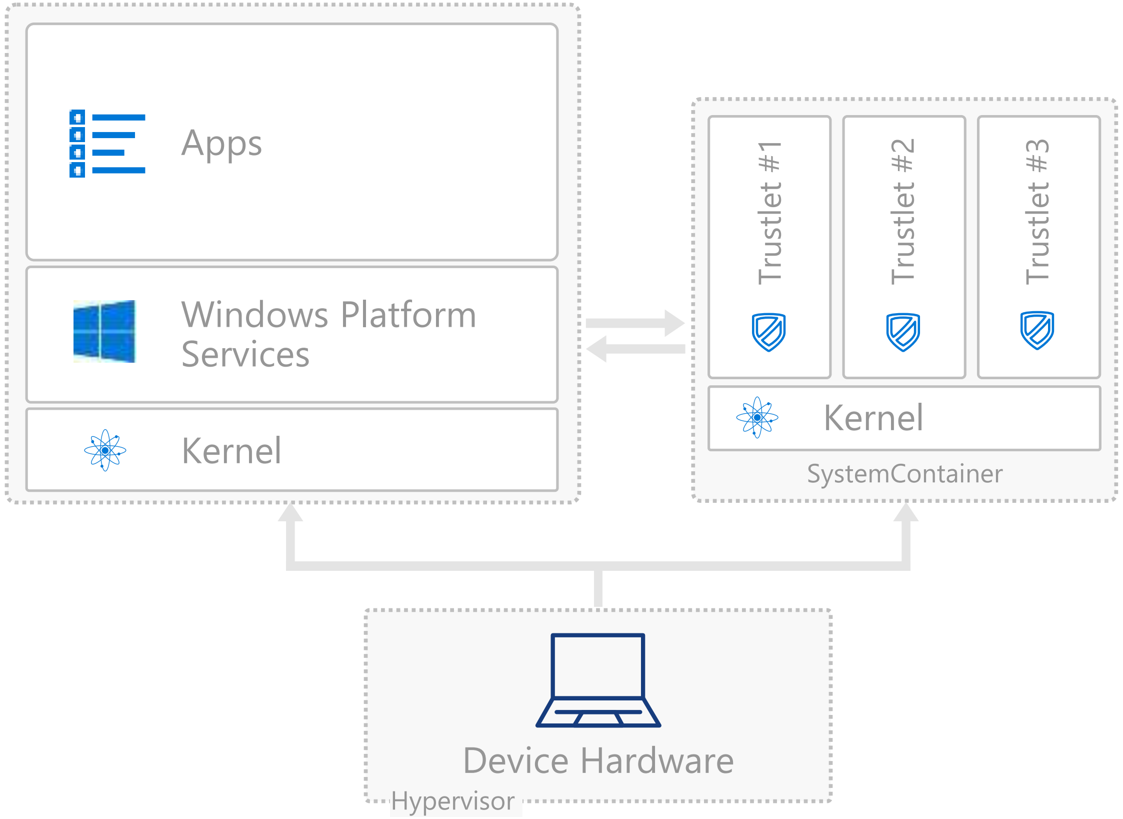
- Hardware generated credential (keys)
- Credential isolated and protected by hardware

Secure biometrics

- Hardened biometric implementation in Windows & hardware
- Anti-spoofing and brute-force protection

HOW WINDOWS PROTECTS
SINGLE SIGN-IN TOKENS

- #1 go-to attack for hackers: Pass the Hash
- Used in nearly every major breach for lateral movement
- Credential Guard uses Windows Defender System Guard to hardware isolate authentication and authentication data away from system
- Fundamentally breaks derived credential theft even when OS is fully compromised



What else?

- Improved Command line
- Hyper-V (Session: What’s new in Microsoft Hyper-V 2016 and 1709)
- MDM for Windows 10 desktop editions
- Windows Subsystem for Linux (WSL)
- Windows Information Protection
- Azure AD join

Resources

- https://docs.microsoft.com/en-us/windows/whats-new/whats-new-windows-10-version-1507-and-1511
- https://docs.microsoft.com/en-us/windows/whats-new/whats-new-windows-10-version-1607
- https://docs.microsoft.com/en-us/windows/whats-new/whats-new-windows-10-version-1703
- https://docs.microsoft.com/en-us/windows/whats-new/whats-new-windows-10-version-1709

Follow-up sessions

- Session: Bezpečný počítač a kde ho najít
  - Windows Defender Antivirus
  - Windows Defender Exploit Guard
  - Windows Defender Application Guard
  - Windows Defender Application Control
- Session: Detekce pokročilých a cílených útoků na počítač
  - Windows Defender Advanced Threat Protection

Dotazy

Kamil Roman

MCSE: Mobility | MCSE: Cloud Platform and Infrastructure | MCSA | MCITP | MCT

konzultace@KamilRT.net

@KamilRT