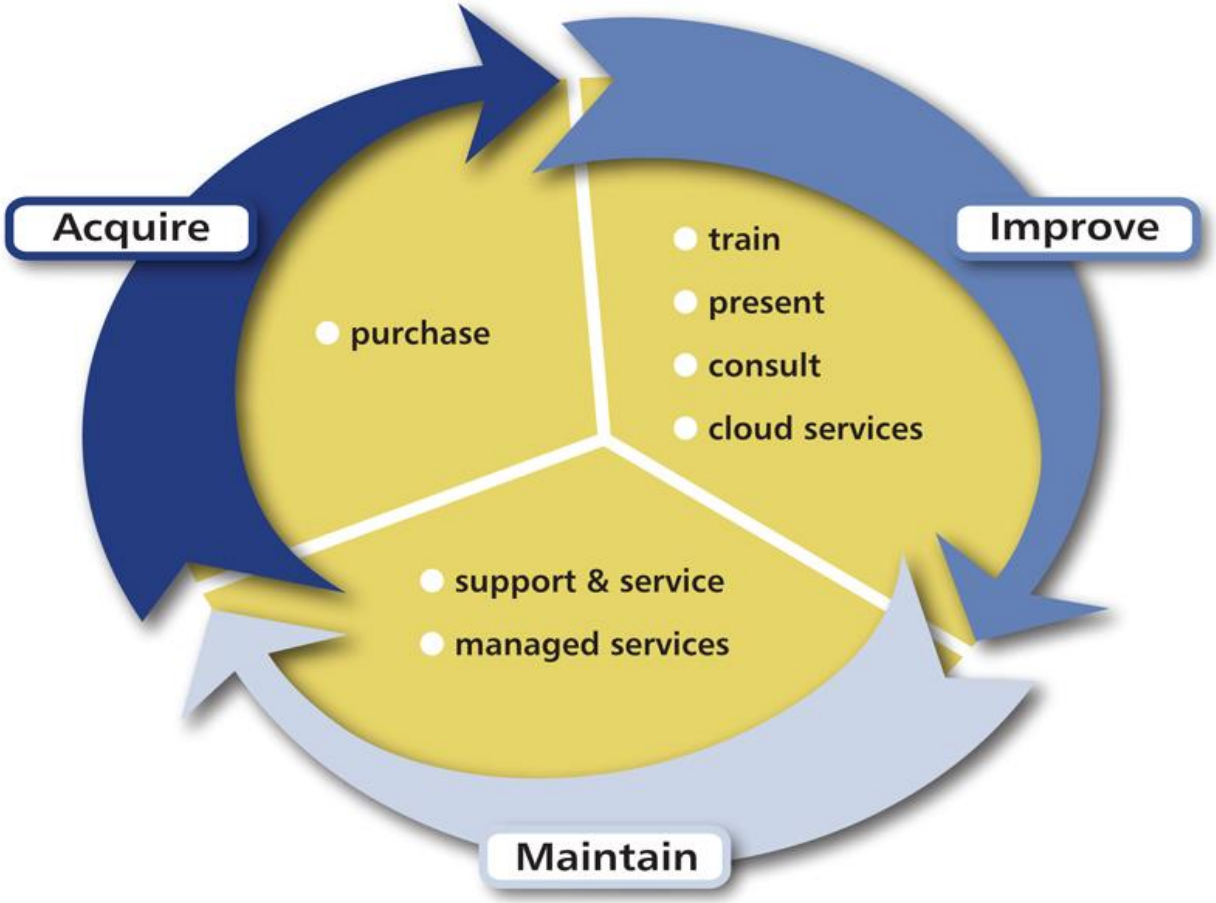
Microsoft® First Look Clinic

40336A

Windows® 10

For IT Professionals

Microsoft



system | source

the one source for IT & AV

System Source & Microsoft:

- **Microsoft Certified Partner…since 1980's**
  - **Silver – Learning Solutions**
    - Train 6,000 students/year
    - Our Instructors rate 20% higher than Microsoft National Average Customer Satisfaction Scores.
  - **Silver – Infrastructure**
- **1,000's of Microsoft implementations**
  - **Small Business to Enterprise**
  - **Non-profit**
  - **Education**

System Source & Microsoft:

- **Microsoft Competencies:**
  - **Server Platform**
    - Microsoft Server 2012
  - **Management & Virtualization**
    - Microsoft Cloud Solutions, Microsoft Private Cloud, System Center, Windows Server
  - **Messaging**
    - Exchange Server, Exchange Online, Forefront Online for Exchange, Forefront Protection 2010 for Exchange Server
  - **Hosting**
    - Exchange Server, SQL Server, Microsoft Server
  - **Devices & Deployment**
    - Windows 8, Office
  - **Small Business**
    - Office 365, Windows 8
  - **Mid Market Solutions Provider**
    - Microsoft Cloud Solutions, Office 365, Office, Windows Server 2012, Windows 8

About This Clinic

This First Look Clinic introduces IT Professionals to the new features and capabilities of Windows 10, using the ***Enterprise Edition*** of Windows 10.

It also covers the key Windows 10 ecosystems of Identity Management, cloud services like Azure Active Directory (AAD), deployment/management tools, and the new User Interface.

No topic is covered in depth, but you will finish the clinic with an understanding of the new features and capabilities of Windows 10 and related services and administration tools.

Clinic Outline

- Module 1: Overview of Windows 10
- Module 2: Deployment and Management of Windows 10
- Module 3: Security Features of Windows 10

Module 1

Overview of Windows 10

Module Overview

- Introduction to Windows 10
- Implementing Windows 10

Topic 1 of 2: Introduction to Windows 10

- Overview of Windows 10 Features that Increase Business Productivity
- New Features of Windows 10
- Windows 10 Features not Available with the Initial Release
- Hands-on Demo: Exploring the new User Interface (UI) of Windows 10

Overview of New Windows 10 Features that Increase Business Productivity

Windows 10 investments for business

Protection against modern security threats

Hardware based security for better malware protection.
Secure boot
Virtual Secure Mode

Secure corporate identity to protect against modern threats.
Microsoft Passport
Biometrics

Protect your corporate data, wherever the data is.
Enterprise data protection (mobile and desktop, with Universal Office and Office for desktop support)

Eliminate malware on your devices.
Device Guard

More secure per-app connection for mobile workers.
Secure Remote Connection

Managed for continuous innovation

Choose management solutions that work best for you.
Mobile Device Management
Group Policy

End of wipe and replace deployment.
Dynamic provisioning
In-place upgrade

Power your business with Universal Apps.
Private catalog
Azure AD Join (desktop and phone)
Business Store

Keep your devices secure and up to date with latest technology.
Delivering Windows as a service

Be more productive

A familiar user experience that adapts to your device.
Start menu
Continuum

Apps that can run on any Windows device.
Universal Apps for Windows

The best productivity experience across all Windows devices.
Office for Windows

Modernize your web experience, stay compatible.
Project "Spartan"
Internet Explorer 11

Innovative devices for your business

Latest Windows innovations on your existing PC fleet.
Great mouse & keyboard support
Hardware compatibility
Granular UX Control

Choose from the range of innovative Windows devices.
2-in-1 devices
Surface
Lumia

Redefine productivity with revolutionary Windows devices.
Surface Hub
HoloLense

Overview of New Features

- Start menu
- Virtual desktops
- *Quick Access* tools menu
- Snap windows to quadrants
- InstantGo
- Device Guard
- Windows Hello
- Universal apps / resizable windows
- Continuum for tablets
- Edge and IE 11
- Cortana virtual assistant
- Credential Guard / VSM
- Microsoft Passport
- Data Leakage Prevention

New Features of Windows 10

Windows 10: the next chapter

One ecosystem for the future

One operating system

One Windows core for all devices

User experience tailored for each device

One developer platform

Universal apps run on every Windows 10 device

One store

Global distribution with local monetization

Reaching over one billion devices

Windows as a service

Delivering innovation on your terms

...and it's still Windows...

Your existing code still works

Management Choices

Identity	Management	Deploying Updates	Infrastructure	Device Ownership
• Active Directory	• Group Policy	• Windows Update	• On-premises	• Corporate-owned
• Azure Active Directory	• System Center Configuration Manager	• Windows Update for Business	• In the cloud	• CYOD
	• 3rd party PC management	• Windows Server Update Services (WSUS)	• Hybrid	• BYOD
	• Intune	• Intune		
	• 3rd party MDM	• 3rd party MDM		

Organizations may mix and match, depending on their specific scenario

Security Enhancements

Leverage Enterprise-grade security

	Windows 7	Windows 10
Identity protection	Reliant on passwords Credential is easy to steal	Secure and easy to deploy multifactor credentials Mainstream use of biometrics on Windows Pass the Hash mitigations Windows Hello Microsoft Passport Enterprise Credential Protection
Data protection	Manual provisioning of drive encryption Data loss prevention requires additional software	Automatic disk encryption and fully integrated data loss prevention BitLocker Enterprise data protection RMS (with Azure)
Threat resistance	Apps are trusted until threat detected Anti-Virus can't keep up with rate of new threats	Device configured to only run trustworthy apps System defenses resilient and protected through isolation Device Guard Windows Defender Hardware Based Isolation
Device security	Platform secured in software	Hardware protection form power on to off UEFI Secure Boot, TPM 2.0 Device Guard

Windows 10 Features made available after the initial release

The following features of Windows 10 were made available after its initial release using a new concept called ***Windows as a Service (more on this later)***:

- Microsoft Passport integration with on premises Active Directory
- Data Leakage Prevention (DLP)
- Windows Store for Business

Demonstration: Exploring the new User Interface (UI) of Windows 10

In this hands-on demo, we will:

- Learn the key features of the new Windows 10 UI
- Use the new Start Screen and Menu
- How to configure and use Cortana
- Use Action Center functionality
- Use IE 11 and the new Edge Browser
- How to use Task View and multiple desktops
- Enhanced SNAP Feature

Topic 2 of 2: Implementing Windows 10

- Windows 10 Desktop and Tablet Editions
- Windows 10 Hardware Requirements

Windows 10 Desktop and Tablet Editions

Desktop features placemat

	Home	Pro	Enterprise
Existing Differentiated Features in Win7 /Win8.1			
Domain Join and Group Policy Management		✓	✓
Existing Win7 / Win 8.1 Enterprise features			✓
Windows 10: Management and Deployment			
Side-loading of LOB apps	✓	✓	✓
MDM Enablement	✓	✓	✓
Ability to join Azure Active Directory		✓	✓
Business Store for Windows 10		✓	✓
Easy Upgrade from Pro to Enterprise edition		✓	✓
Granular UX Control			✓
Windows 10: Security			
Microsoft Passport	✓	✓	✓
Enterprise Data Protection		✓	✓
Credential Guard			✓
Device Guard			✓
Windows 10: Windows as a Service, Support & Entitlements			
Windows Update for Business & Current Branch for Business		✓	✓
Access to Long Term Servicing Branch			✓

Windows 10 Hardware Requirements

Windows 10 minimum Hardware requirements (Desktop editions):

- Processor: 1 GHz or faster
- RAM: 1 GB (32-bit) or 2 GB (64-bit)
- Free hard disk space: 16 GB
- Graphics card: Microsoft DirectX 9 graphics device with WDDM driver
- Some features have additional requirements:
  - **For Full BitLocker support:** Trusted Platform Module (TPM) 1.2 or newer
  - **For Secure Boot**: Unified Extensible Firmware Interface (UEFI)-based BIOS
  - **For Client Hyper-V:** SLAT, Processor-assisted virtualization
  - **For Credential Guard**: Secure boot and Hyper-V enabled, TPM 1.2 or newe
  - **For Windows Hello facial recognition**: *Intel RealSense-supported camera*

Windows 10 Requirements for Mobile Hardware

Windows 10 requirements for (Mobile editions):

- Minimum 3 inch screen
- Memory: 512 MB for 32-bit OS
- Storage Space: 4GB
- Graphics: DirectX 9 with the following RAM requirements based on resolution:
- 512MB of RAM for:
  - ***Full Wide VGA (FGVGA) (854x480 pixels)***
  - ***Wide VGA (WVGA) (800x480 pixels)***
- 1GB of RAM for:
  - ***Wide Super VGA (WSVGA) (1024x600 pixels)***
  - ***HD (1280x720 pixels)***
  - ***Wide XGA (WXGA) (1366x768 pixels)***
  - ***Quarter High Definition (qHD) (960x540 pixels)***
- 2GB of RAM for:
  - ***Full-HD (1920x1080 pixels)***

Systems Support for Windows Hello

Windows Hello Features and Requirements:

1. Facial Feature Recognition
    - ***Intel RealSense*** Device must be present:
        - Lenovo Yoga 15
        - Dell Inspiron 15
        - HP Envy 15
        - Intel RealSense Dev Kit

2. Fingerprint Recognition
    - Most Windows 8/8.1 certified fingerprint devices will work

Module Review

- Review Question(s)

Module 2

Deployment and Management of Windows 10

Module Overview

- Deployment of Windows 10
- Provisioning for Windows 10
- Managing Windows 10
- Supporting Windows 10

Topic 1 of 4: Deployment of Windows 10

- Deployment Options
- In-Place Upgrade
- Reasons Why You Should Use an In-Place Upgrade

Deployment Options

Deployment Choices

Wipe-and-Load

Traditional process

- Capture data and settings
- Deploy (custom) OS image
- Inject drivers
- Install apps
- Restore data and settings

Still an option for all scenarios

In-Place

Let Windows do the work

- Preserve all data, settings, apps, drivers
- Install (standard) OS image
- Restore everything

Recommended for existing devices (Windows 7/8/8.1)

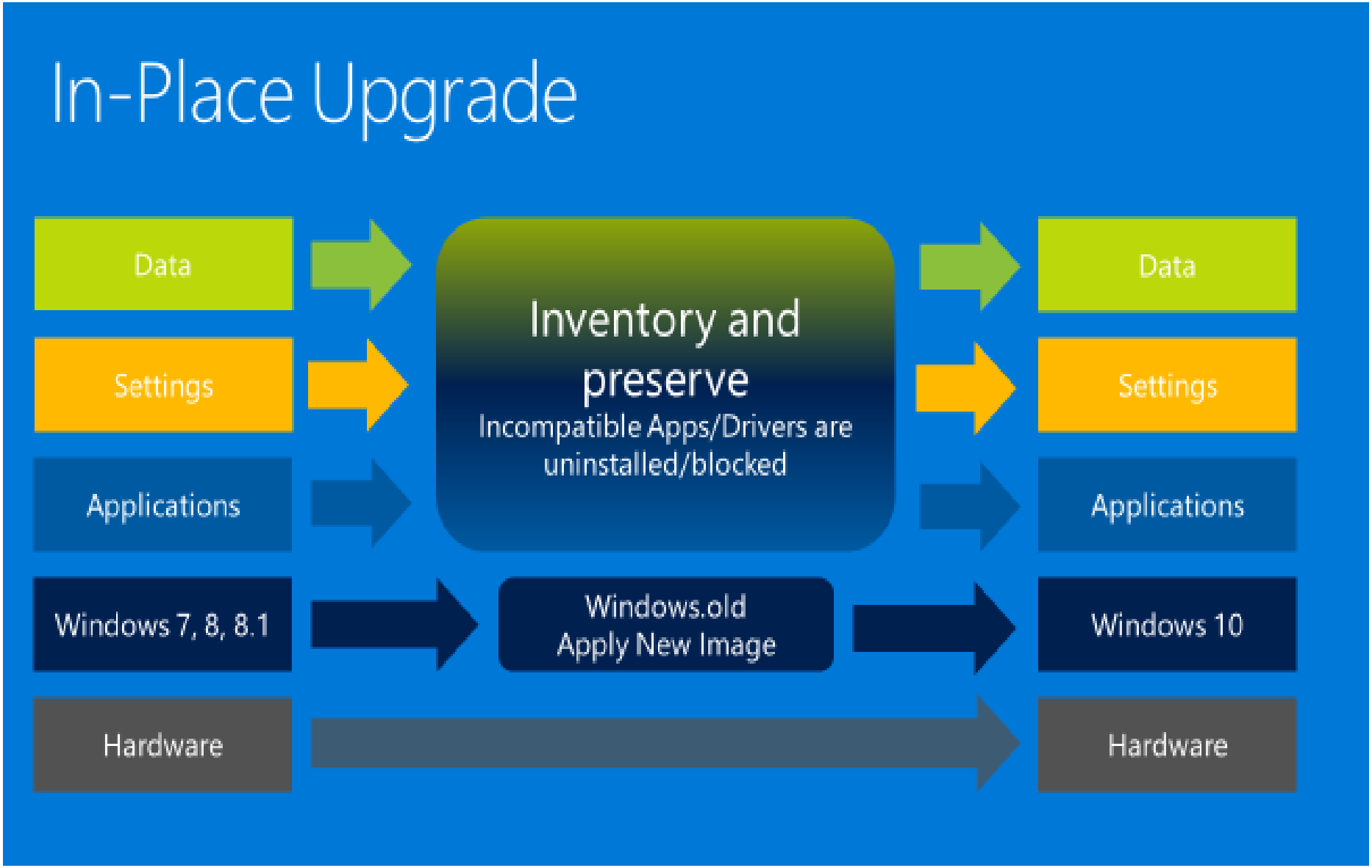
Provisioning

Configure new devices

- Transform into an Enterprise device
- Remove extra items, add organizational apps and config

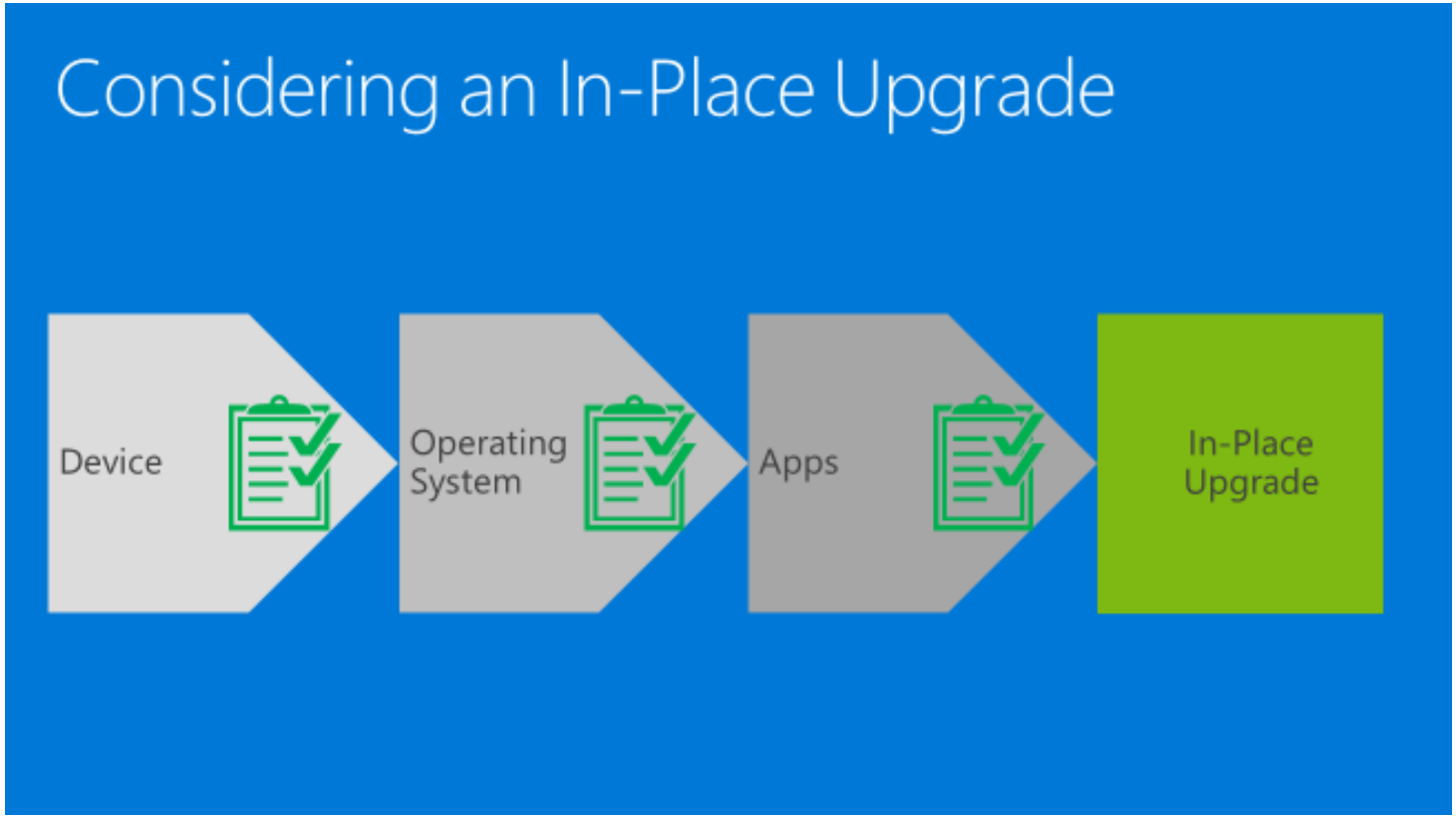
New capability for new devices

In-Place Upgrade

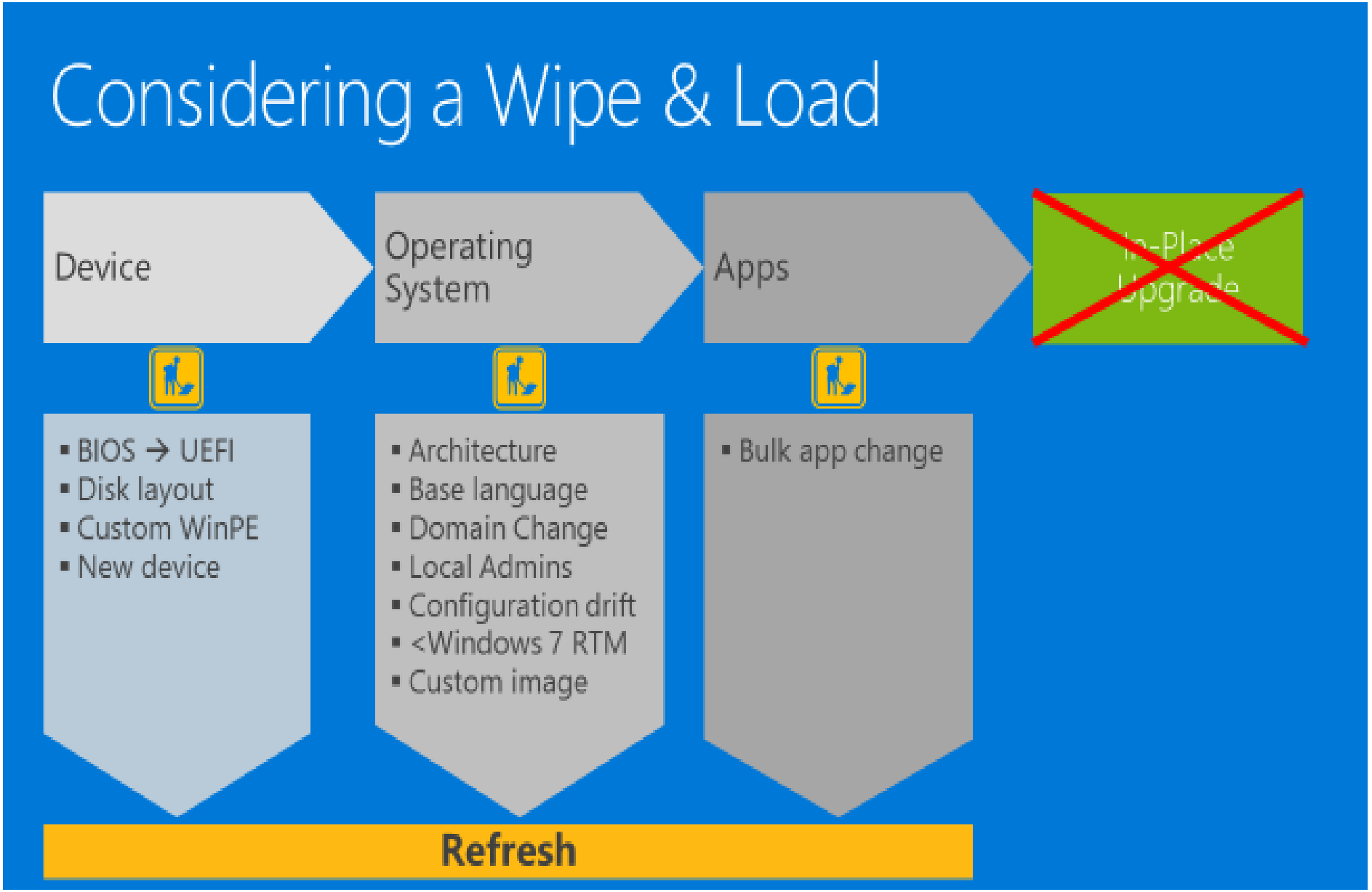


Reasons Why You Should Use an In-Place Upgrade

- Microsoft now recommends that you consider In-Place upgrades to Windows 10 if:
  - Systems meet the hardware requirements of Windows 10
  - Systems are currently running Windows 7, 8 or 8.1
  - Apps have been tested and are compatible with Windows 10



When to use Wipe and Load



Topic 2 of 4: Provisioning for Windows 10

- Windows 10 Provisioning

Windows 10 Provisioning

When to use Provisioning

When to use Provisioning?

1. Configure a device in deployments without MDM
2. Automate enrollment into MDM, Domain or Azure Active Directory
3. Ensure compliance and security BEFORE the device is enrolled

Windows 10 Deployment Scenarios (19 minute video)

Topic 3 of 4: Managing Windows 10

- Windows Management Choices
- Windows Management Features
- Windows 10 Identify Choices

Windows Management Choices

	Available Choices
Identity	Active Directory, Azure Active Directory
Management	Group Policy, System Center Configuration Manager, 3rd party tools
Updates	Windows Update, Windows Server Update Services, Microsoft Intune, 3rd party tools
Infrastructure	On-premises or in the cloud
Ownership	Corporate owned, CYOD, BYOD

Windows Management Features

Windows 10 Works with Existing Infrastructure

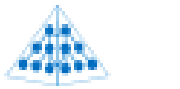
Product	Supports Windows 10 Management	Supports Windows 10 Deployment
System Center 2012 R2 Configuration Manager	✔	✔
System Center 2012 Configuration Manager	✔	✔
System Center Configuration Manager 2007	✔	
Windows Server 2012 R2 Windows Server 2012 Windows Server 2008	✔	
Microsoft Deployment Toolkit 2013		✔

Updates will be required. New OS features may require newer versions for full support.

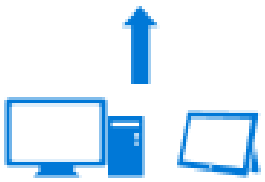
Windows 10 Identify Choices

Windows 10 Identity Choices

Organization Owned

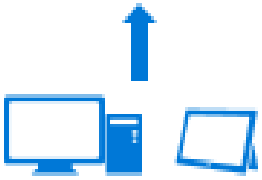


Active Directory



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

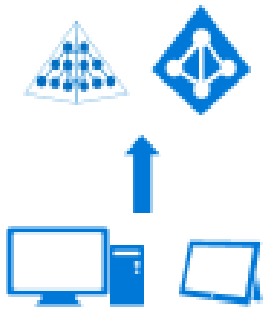
Azure Active Directory



- Computer joins Azure AD to establish trust
- User signs on using Azure AD account
- Intune/MDM
- Settings roaming

Single sign-on to enterprise + cloud-based services

Personally Owned (BYOD)



- Computer registers with AD or Azure AD via **Device Registration** to establish trust for remote resource access
- User signs in with a Microsoft account, associates an Azure AD account
- Intune/MDM

Group Policy & Windows 10

New in Windows 10	New Since Windows 7
New policies to support Windows 10 specific features: • Start Screen and Start Menu management • Edge browser settings • Microsoft Passport credential PIN settings • Universal app management • Device Guard and Credential Guard settings	Capabilities from Windows 8.1 • Local GPO caching for improved boot times with high latency DC connections • IPv6 support for Printers and VPN Capabilities from Windows 8 • Automatic switchover to asynchronous processing for DirectAccess clients when link speed cannot be determined • Maximum size of registry policies (registry.pol) increased to 100 MB • Remote group policy refresh from the GPMC • More efficient background processing: Group Policy client service “sleeps” between background refresh cycles

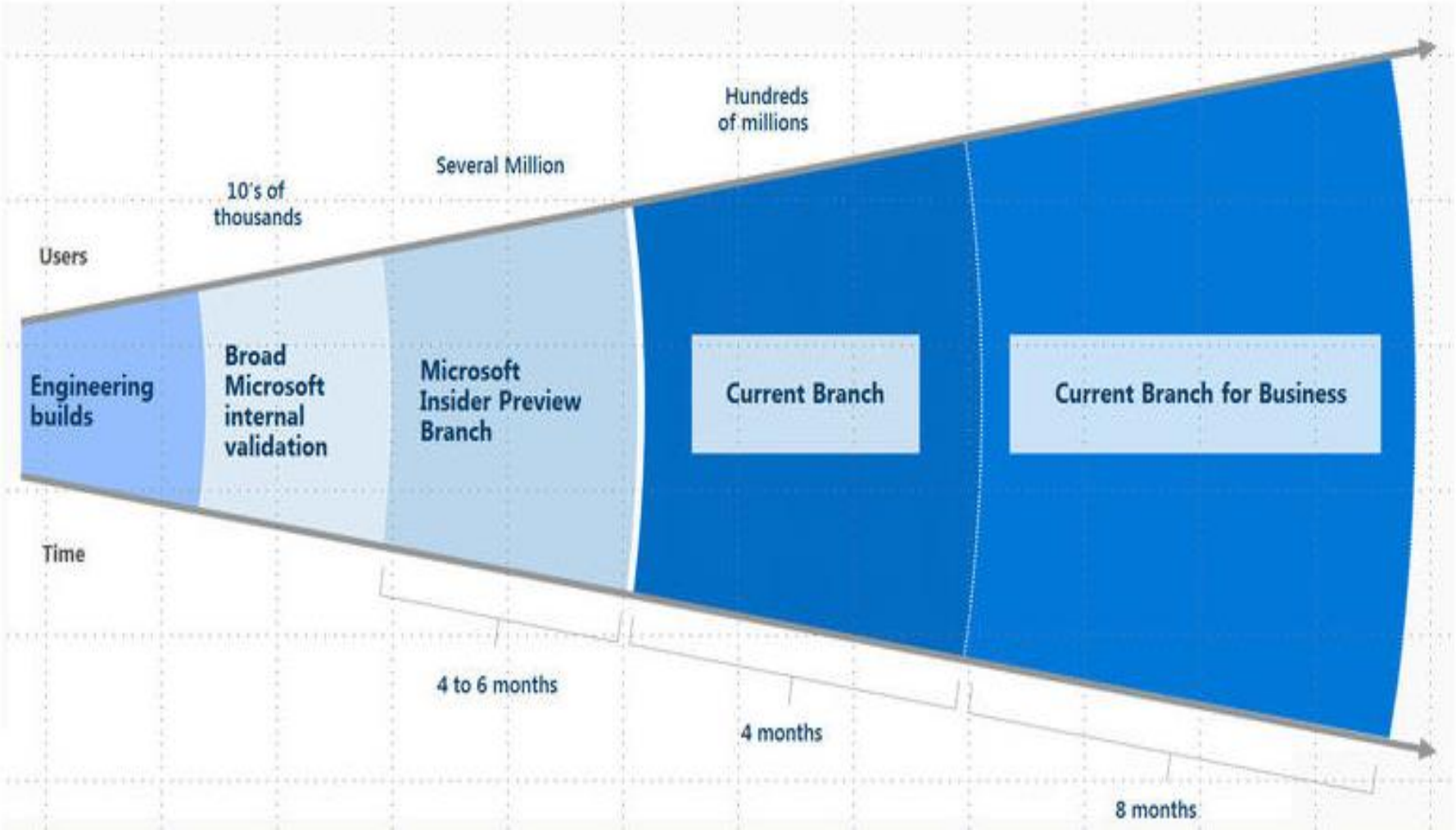
Topic 4 of 4: Supporting Windows 10

- Windows as a Service
- Windows Update for Business
- Current Branch for Business

Windows as a Service

- In today's environment, complete product cycles need to be measured in months, not years
- New releases must be made available on a continual basis, and must be deployable with minimal impact on users
- Microsoft designed Windows 10 to meet these requirements by implementing a new approach to innovation development and delivery called ***Windows as a Service (WaaS)***
- Windows as a Service is based on a community-centric approach involving internal Microsoft engineers, other Microsoft employees, early adopters and others, for testing both:
  - **Feature upgrades:** these include the latest new features, experiences, and capabilities on devices that are already running Windows 10
  - **Servicing updates:** which include security fixes and other important updates
- Upgrades and updates are then released in ***branches*** made up of one or more ***rings***

How the Branches fit together



For excellent in-depth coverage: https://technet.microsoft.com/en-us/library/mt598226(v=vs.85).aspx

Long Term Servicing Branch edition

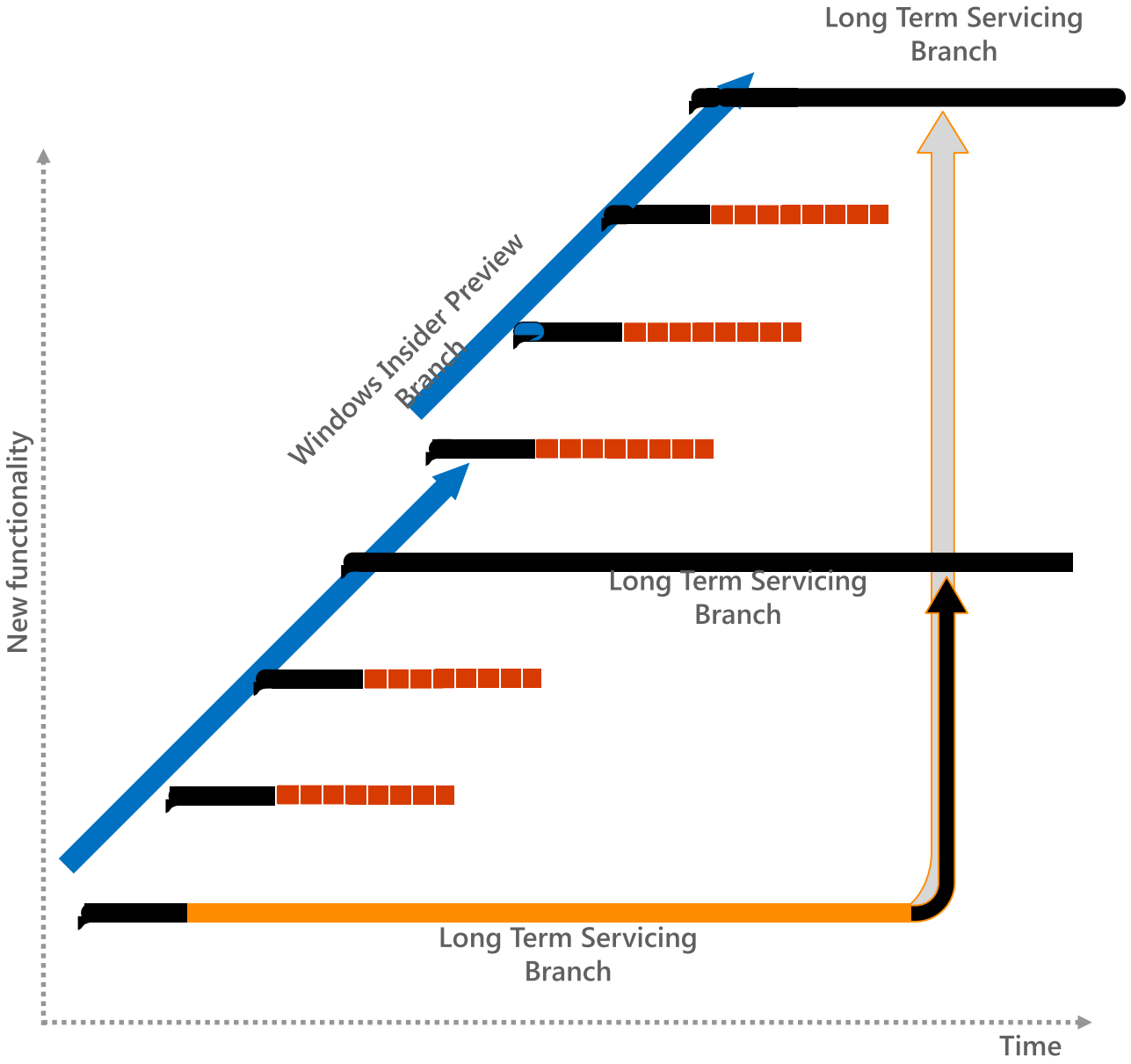
With Windows Enterprise LTSB edition, security updates and fixes are still delivered regularly

Customers on Long Term Servicing Branch receive security and critical fixes for **10 years**

Customers can move from one LTSB to the next one via in-place upgrade and can skip one LTSB as well

LTSB is targeted at special purpose computers where stability is the utmost concern

LTSB is available for Enterprise edition only



Module Review

- Review Question(s)

Module 3

Security Features of Windows 10

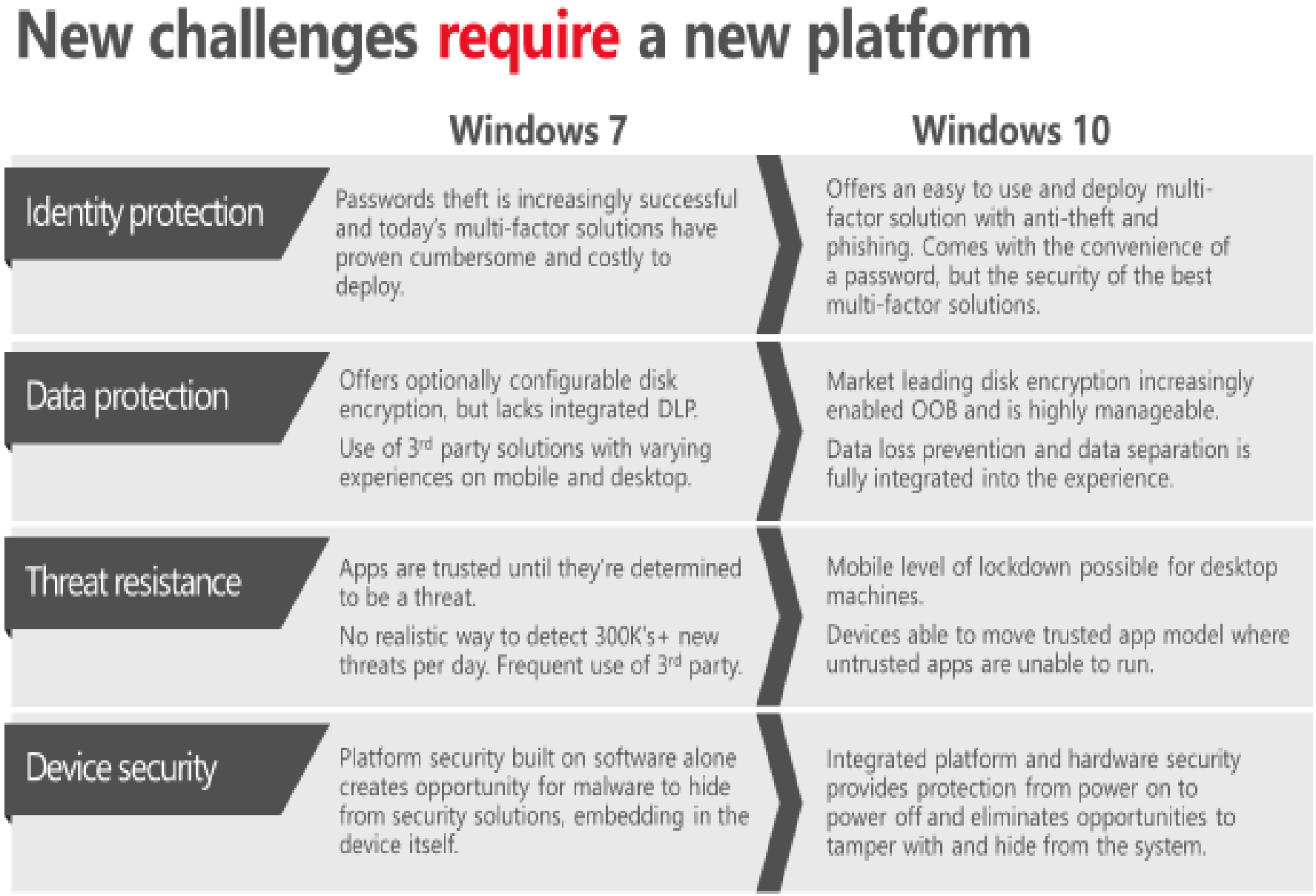
Module Overview

- Windows 10 Security Overview
- Overview of Device Guard

Topic 1 of 2: Windows 10 Security Overview

- New Security Challenges require a new Platform
- Windows SmartScreen
- Demonstration: Configuring Windows SmartScreen Settings
- Configuring Windows Defender
- Demonstration: Configuring Scanning Options in Windows Defender
- Data at Rest Protection – Encryption for the Rest of Us
- Demonstration: BitLocker management

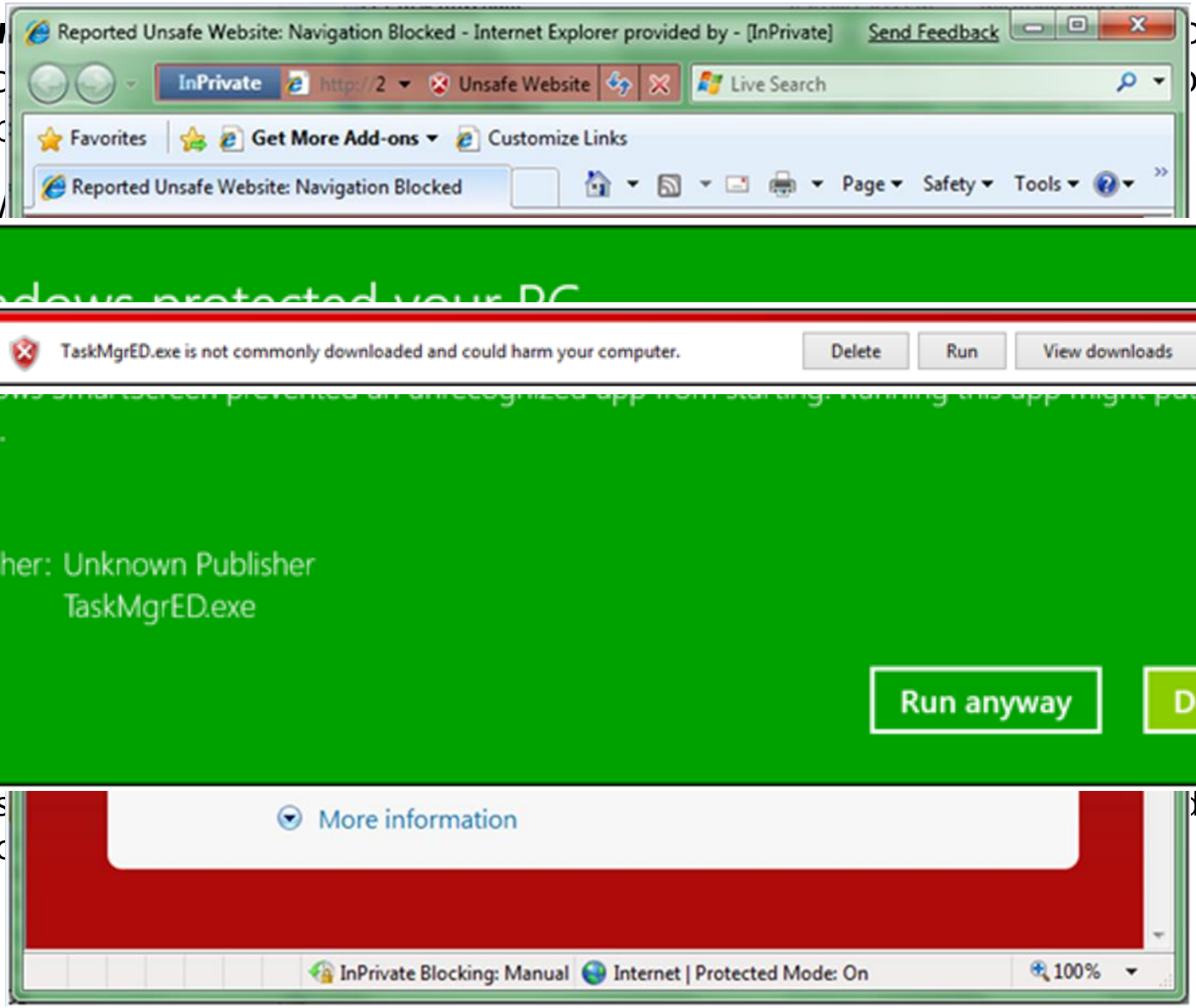
New Security Challenges require a new Platform



Windows SmartScreen

Smar owsing malic on datab

- In V



s d if it is c

Configuring Windows Defender

Windows Defender is an integrated solution that provides protection from spyware, malware and viruses

Is Windows Defender good enough?

Demos: Configuring Windows SmartScreen Settings and Windows Defender

- In this hands-on demo, we will configure Windows SmartScreen and Windows Defender.

Data at Rest Protection with BitLocker

Device Encryption – BitLocker

- Devices can be encrypted out-of-box with BitLocker
- Increased global acceptance of integrating Trusted Platform Module (TPM) hardware in many devices
- Goal: pervasive on all Windows devices by 2016
- Enterprise-grade management when combined with Microsoft BitLocker Administration and Management (MBAM)

Hands-on demo: BitLocker management

- In this demo, we will review options for the BitLocker feature in Windows 10

Topic 2 of 2: Overview of Device Guard

- Configurable code integrity
- Planning for Device Guard
- Device Guard Catalog files
- Demonstration: Using Device Guard

What is Device Guard?

- ***Code integrity*** is the component of Windows that verifies that running code is trusted and safe
- Until now, for non-mobile platforms, code integrity consisted largely of requiring digital signatures on device drivers
- ***Device Guard*** allows non-mobile Windows platforms to function like a mobile phone, letting only specific applications to be trusted and exectued

Planning for Device Guard

Planning for Device Guard:

- **Approaching enterprise code integrity deployment.** Deploying Device Guard to your organization requires a planned and phased-in approach
- **Device Guard deployment scenarios.** As part of planning for Device Guard deployment, Microsoft recommends that you categorize each device in your organization into a deployment scenario
- **Code signing adoption.** Code signing is important to the security that Device Guard provides
- **Hardware considerations.** Several Device Guard features require advanced hardware (note: they are referring here to *Credential Guard* which is not covered in this seminar)

Device Guard Catalog files

Planning for Device Guard:

- Know your targeting group of devices
- Use PowerShell cmdlets to create policy from golden image systems
  - Defaults to Audit Mode
  - Merge multiple policies or Deploy differential policies
- Deploy policy in audit mode and test
- Use Powershell cmdlets to create policy from audit log and merge
- Enable enforcement

Demonstration: Using Device Guard

Implementing a Device Guard Policy involves the newest version of Powershell:

1. Create one or more “Golden Images”
2. On the Golden Image machine, create a code integrity policy with Powershell’s `New-CIPolicy` cmdlet
3. Copy the resulting policy file to a shared folder accessible to targeted systems
4. Configure Group Policy to deploy the settings. The file gets pushed to `c:\windows\system32\CodeIntegrity` on targeted computers and renamed to `SIPolicy.p7b`
5. Restart the computer

Windows 10 Training

Windows 10 Training at System Source

- 20697-1: Installing and Configuring Windows 10
  - April 18-22 in Hunt Valley
  - May 16-20 in Columbia
- 20697-2: Deploying and Managing Windows 10 Using Enterprise Services
  - May 23-17 in Columbia
  - July 25-29 in Columbia
- 10982: Supporting and Troubleshooting Windows 10
  - May 16-20 in Columbia
  - August 15-19 in Hunt Valley

Clinic Evaluation