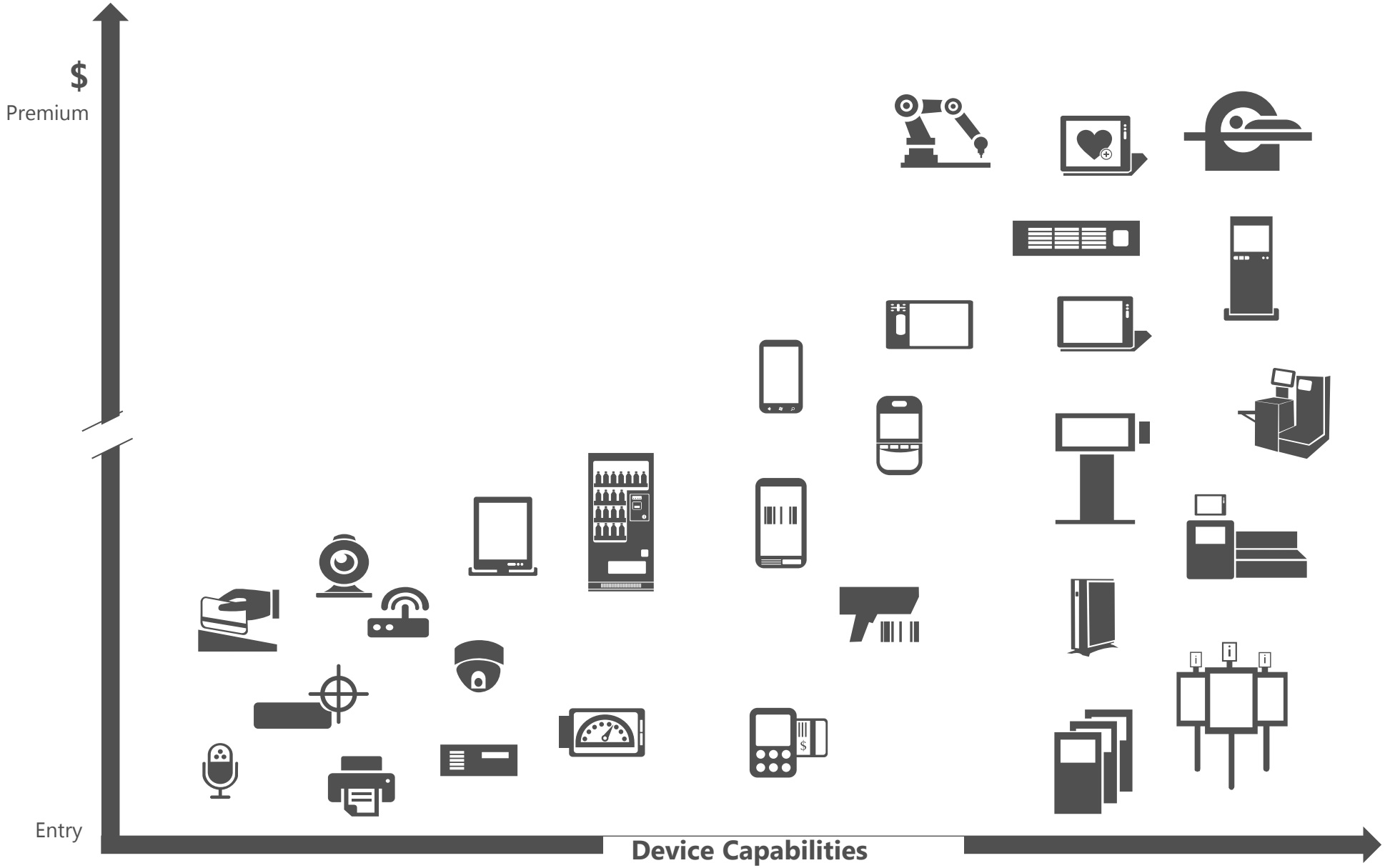
Windows 10 IoT Enterprise overview & security

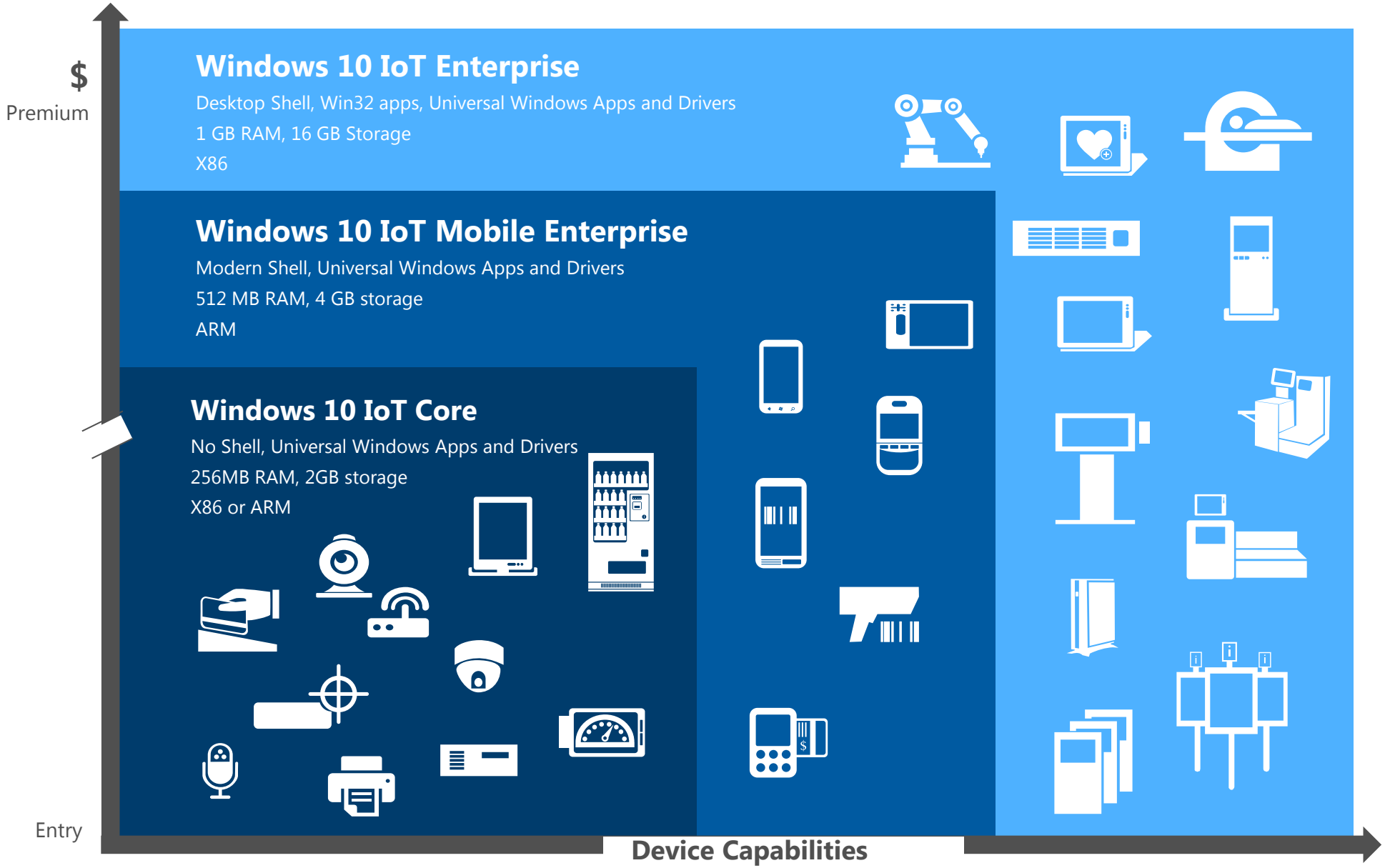
Michal Lichtman Cohen
Eastronics

What is Microsoft Embedded?

Windows Devices



Windows 10 IoT



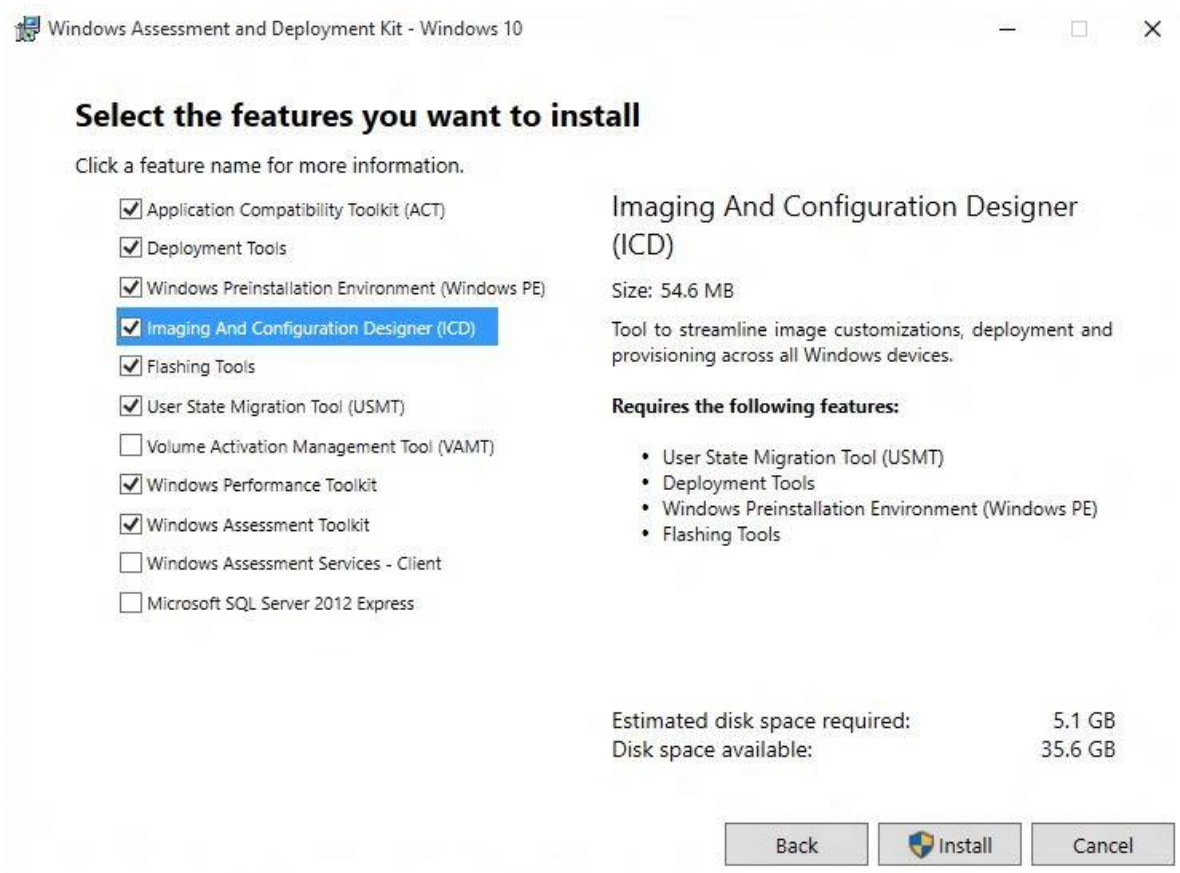
Windows Assessment and Deployment Kit (ADK)

Windows Assessment Toolkit

Windows Performance Toolkit

NEW

Windows Imaging and Configuration Designer



MICROSOFT'S COMPREHENSIVE **VISION** FOR SECURITY

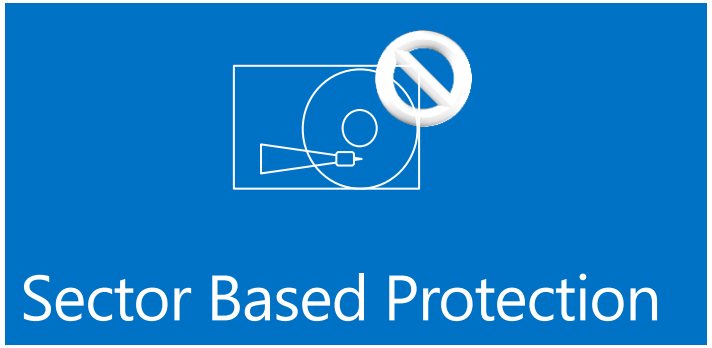
	Protect	Detect	Respond
Devices	Protect across levels – Hardware, Software, and Applications	Detect any deviations from baseline, policies, or behavior	Respond dynamically to any suspicious devices
Apps	Protect apps using platform features that defend and reduce attack surface area	Detect use of unsanctioned apps or threats against apps	Respond dynamically to any suspicious applications and behavior
Users	Protect by reducing threat of credential theft	Detect suspicious behavior and unusual activity	Respond by elevating access requirements based on risk
Data	Protect data no matter where it is located	Detect any attempts for unauthorized data access	Respond to any data leak by removing and monitoring access

Windows 10 Security

Device protection	Threat resistance	Identity protection	Information protection	Breach detection investigation & response
Virtualization Based Security				
UEFI Secure Boot	Device Guard		Device Encryption	
Windows Trusted Boot	Windows Defender Application Guard for Microsoft Edge	Credential Guard	Windows Information Protection	Security Management
Windows Update	Microsoft Edge	Windows Hello Companion Devices	BitLocker Admin and Monitoring	Conditional Access
	Windows Defender			
Trusted Platform Module	Windows Firewall	Windows Hello	BitLocker	Windows Defender Advanced Threat Protection
	SmartScreen		BitLocker to Go	

PRE-BREACH → POST-BREACH

Unified Write Filter (UWF)



Create read only devices

Protect system against write operations

Improve system up-time

Reduce IT support & improve compliance

Restrict Access to USB Devices

Group Policy or ICD

Prevent installation of all devices

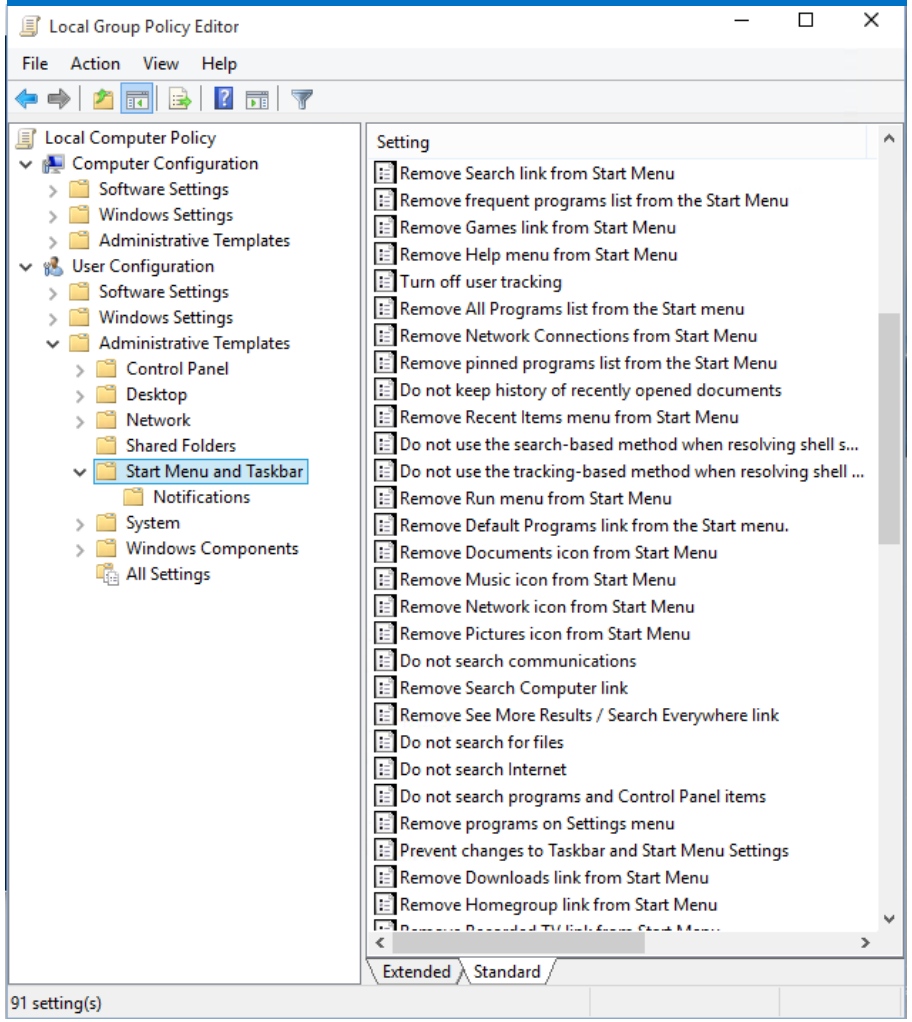
Allow users to install only authorized devices

Prevent installation of prohibited devices

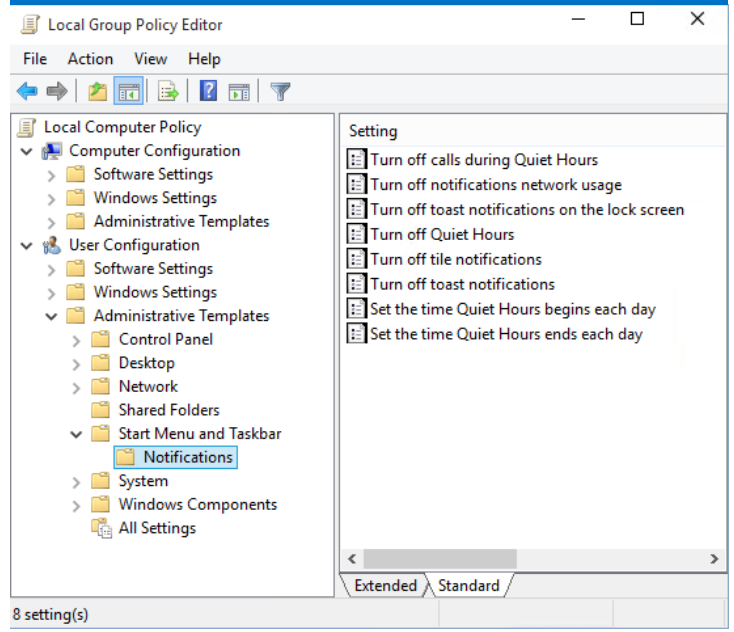
Control read and write permissions on removable media

Granular UX Control | Group Policy, ICD or SIM

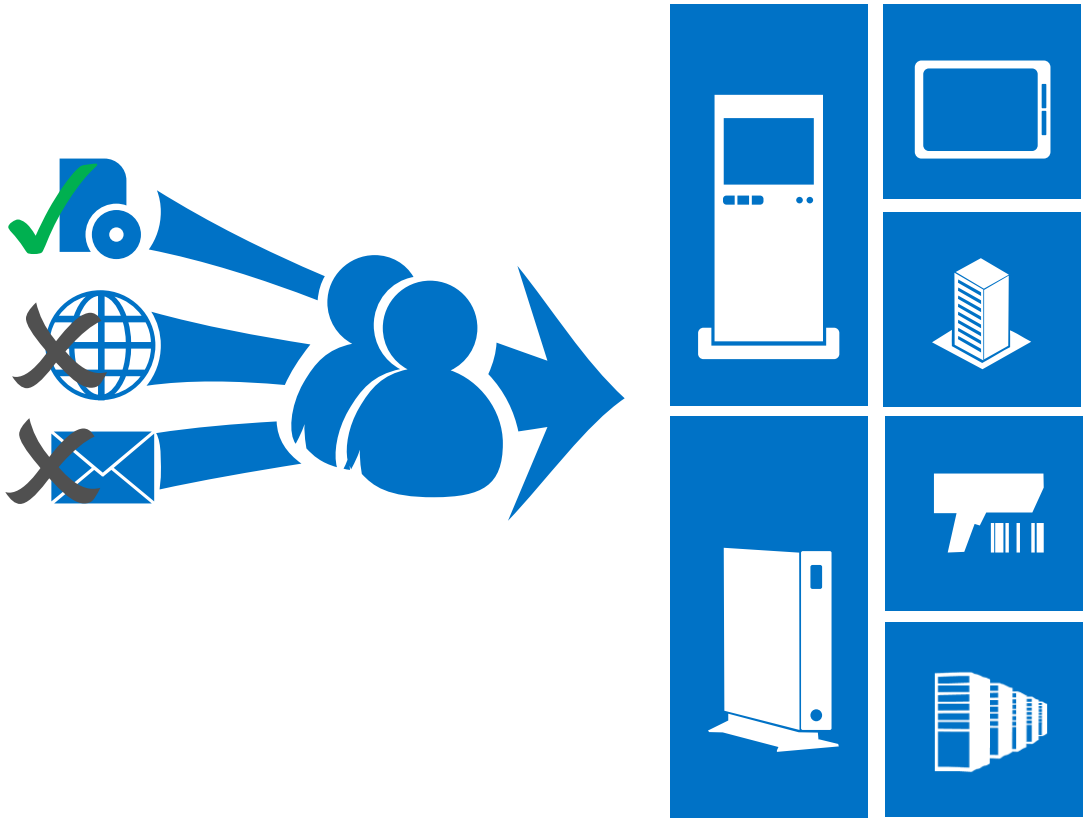
Fully customize the Start Menu, Start Screen taskbar to a desired layout



Suppress toast notifications



AppLocker



Eliminate unwanted/unknown applications in your network

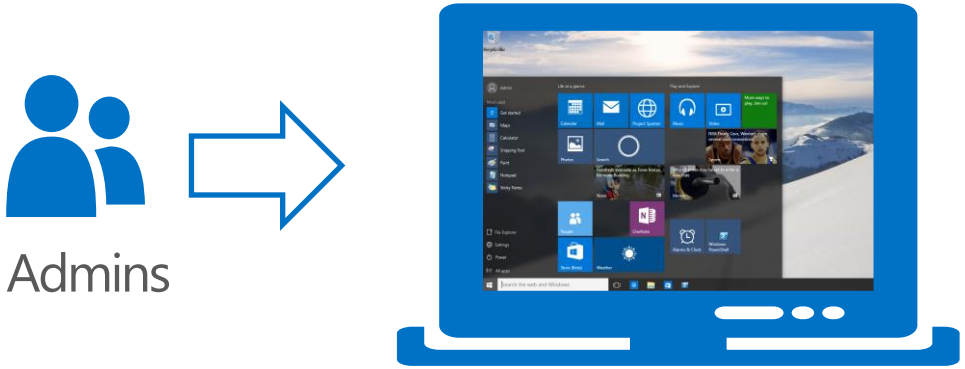
Enforce application standardization within your organization

Easily create and manage flexible rules using Group Policy

Shell Launcher

Launch Classic Windows apps as a custom shell

Dedicated device & app experience



Different shells for different user groups

Admins can still have access to the Universal Windows Platform

DEVICE GUARD

Hardware Rooted App Control

Windows desktop can be locked down to only run trusted apps, just like many mobile OS's

Untrusted apps and executables, such as malware, are unable to run

Signed policy secures configuration from tampering

Protects system core (kernel mode) and drivers from zero days and vulnerabilities

Requires hardware with VT-X and VT-D

Supports all apps including Universal and Desktop (Win32).

Trusted apps can be created by IHV, ISV, and organizations using a Microsoft provided signing service.

Apps and policies must be signed. No additional modification is required.

Signing service for policies available to enterprises on the Windows Store for Business.

Device Guard

The Parts to the Solution

Hardware security

Configurable code integrity

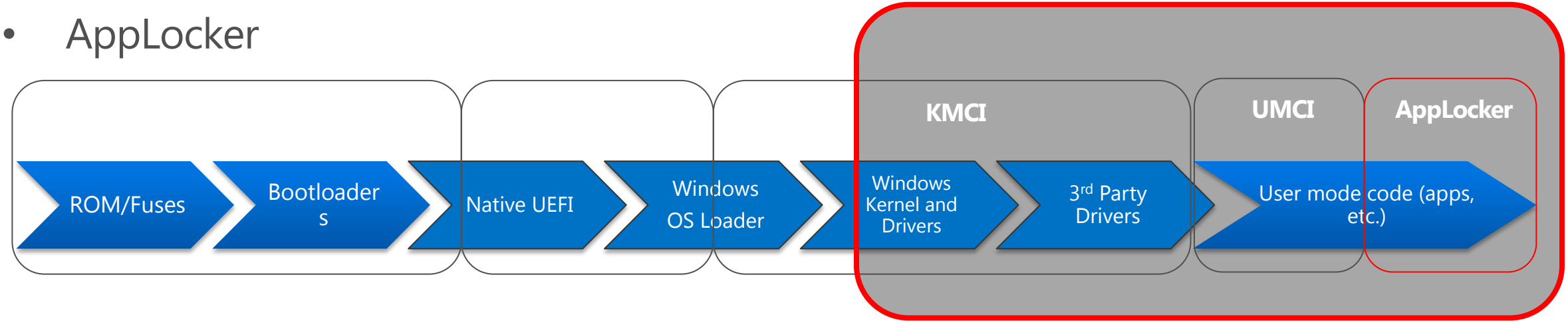
Virtualization based security

- Protects critical parts of the OS against admin/kernel level malware

Manageability via GP or PowerShell

Code Integrity

- Secure Boot
  - Includes Secure Firmware Updates and Platform Secure Boot
- Kernel Mode Code Integrity (KMCI)
- User Mode Code Integrity (UMCI)
- Early Launch Anti-Malware
- AppLocker



Virtualization Based Security

Provides a new trust boundary for system software

- Leverage platform virtualization to enhance platform security
- Limit access to high-value security assets from supervisor mode (CPL0) code

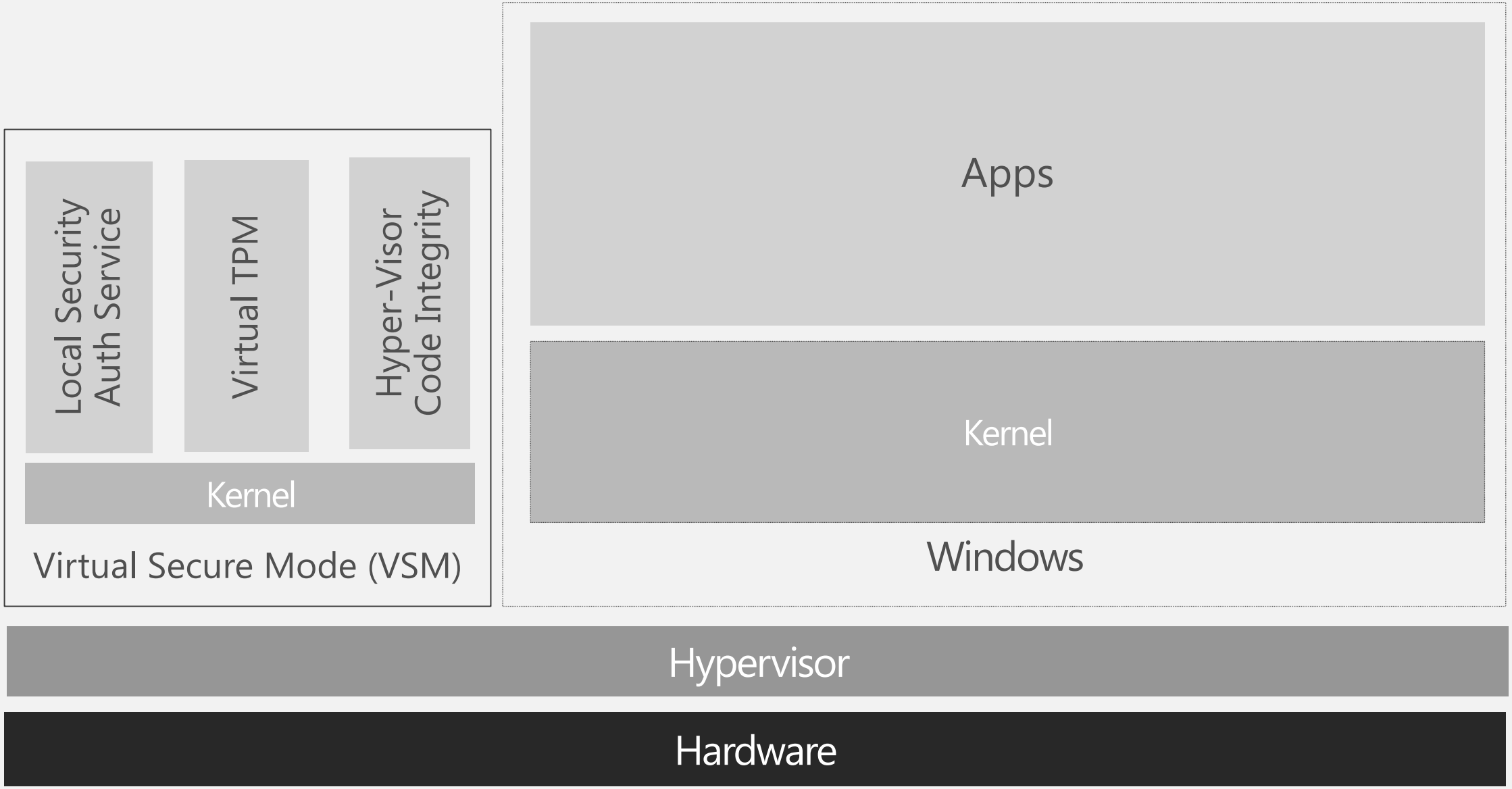
Provides a secure execution environment to enable:

- Protected storage and management of platform security assets
- Enhanced OS protection against attacks (including attacks from kernel-mode)
- A basis for strengthening protections of guest VM secrets from the host OS

Windows 10 services protected with virtualization based security

- LSA Credential Isolation (Local Security Authority)
- vTPM (server only)
- Kernel Mode Code Integrity (KMCI)

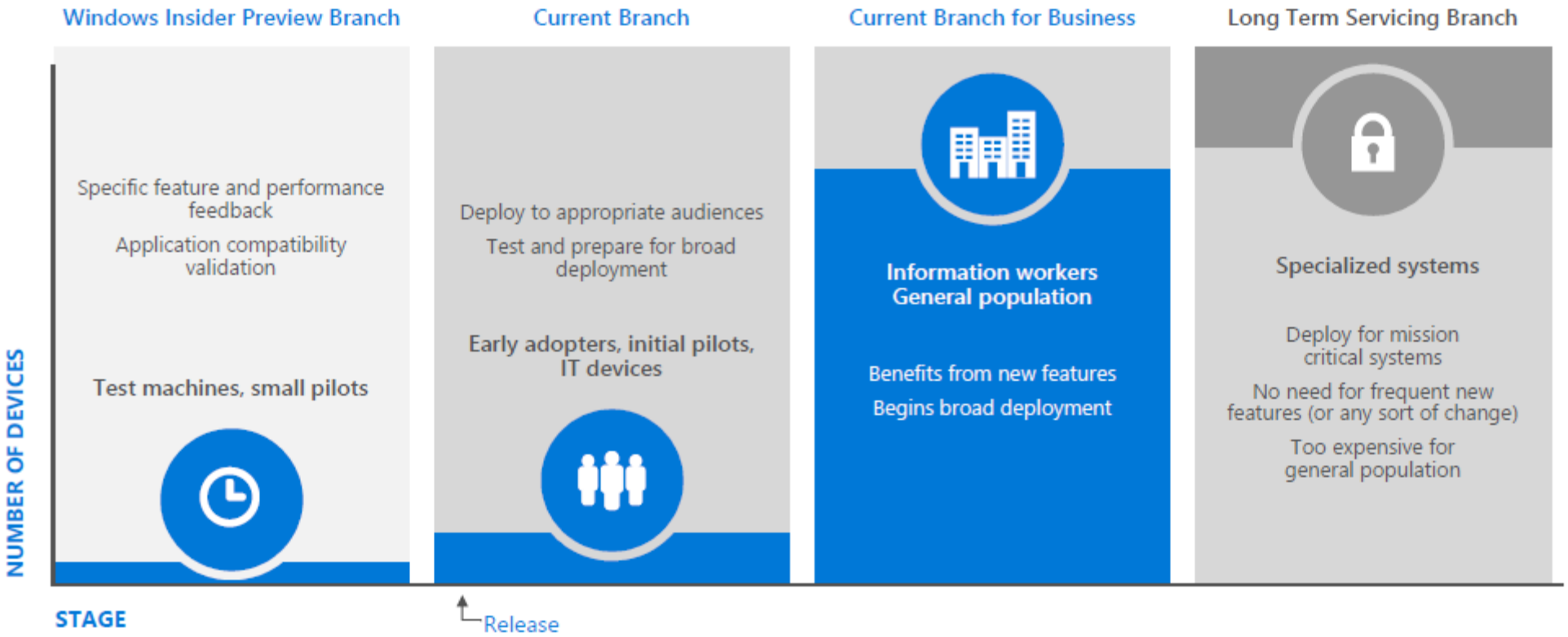
Code Integrity protected by VSM



Lets switch to a short introduction to Windows 10 IOT tools and setting

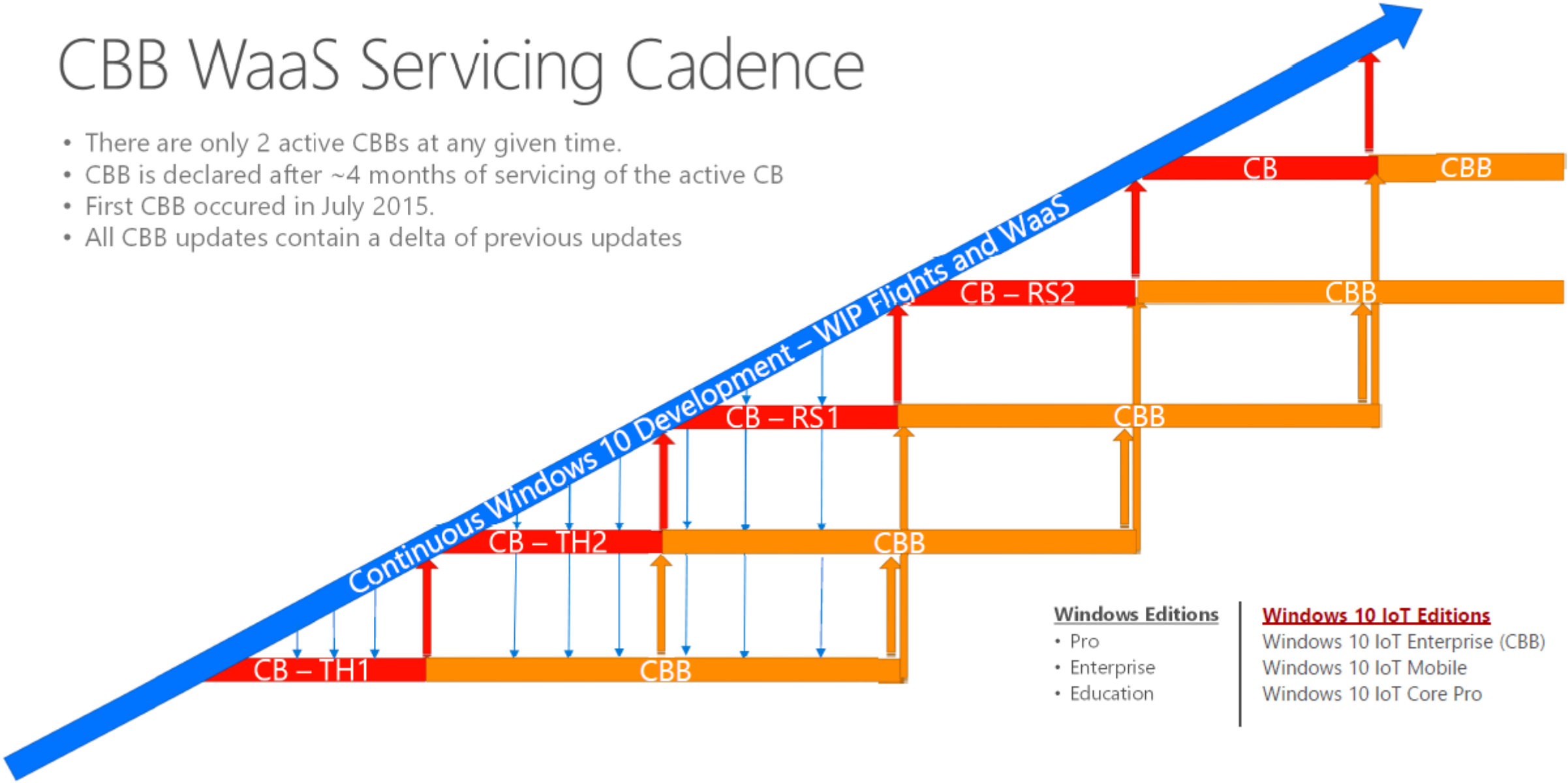
Windows as a service: Deploying Windows

Unmatched flexibility and control, depending on needs



CBB WaaS Servicing Cadence

- There are only 2 active CBBs at any given time.
- CBB is declared after ~4 months of servicing of the active CB
- First CBB occured in July 2015.
- All CBB updates contain a delta of previous updates

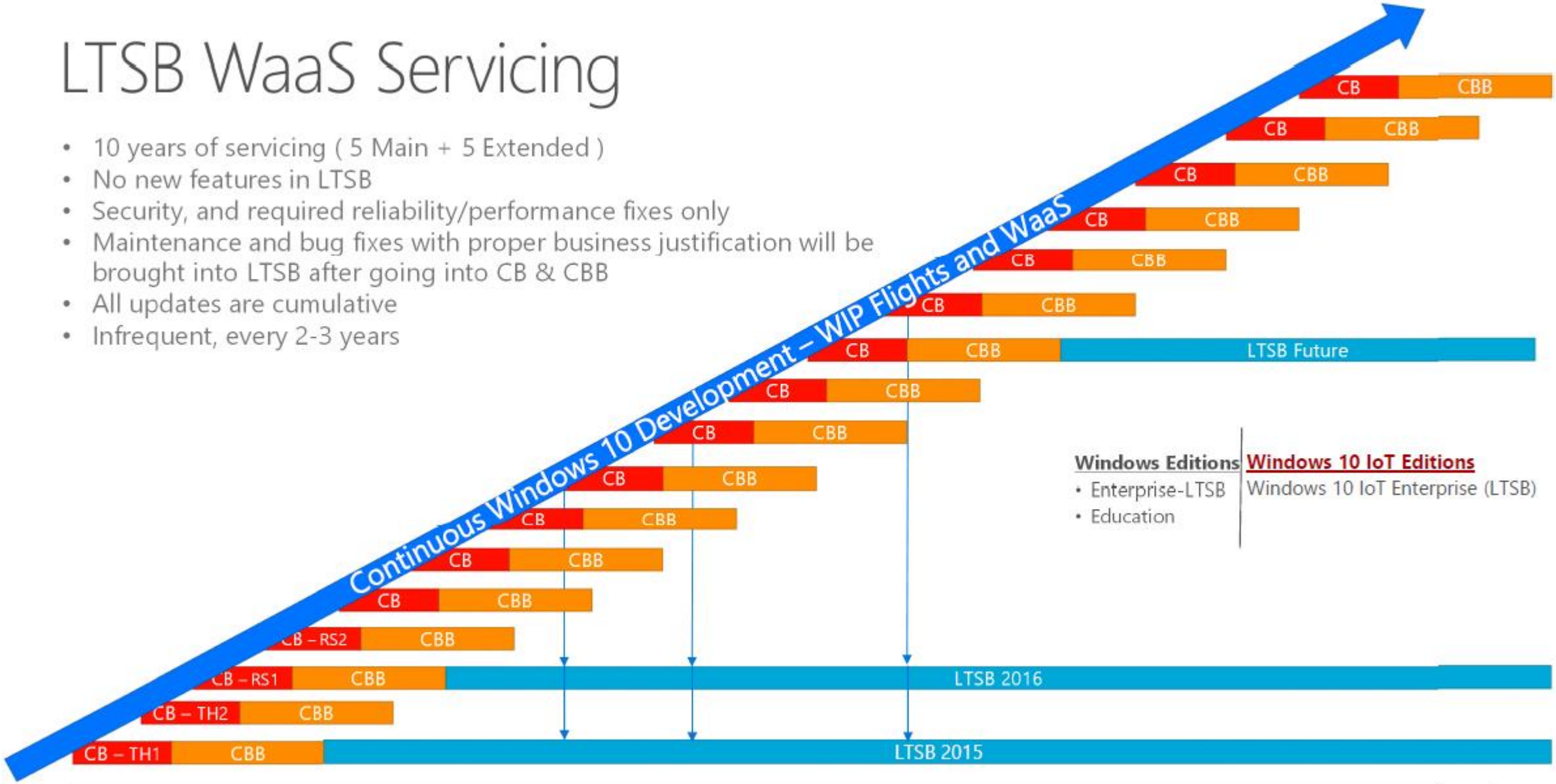


Windows Editions
- Pro
- Enterprise
- Education

Windows 10 IoT Editions
Windows 10 IoT Enterprise (CBB)
Windows 10 IoT Mobile
Windows 10 IoT Core Pro

LTSB WaaS Servicing

- 10 years of servicing (5 Main + 5 Extended)
- No new features in LTSB
- Security, and required reliability/performance fixes only
- Maintenance and bug fixes with proper business justification will be brought into LTSB after going into CB & CBB
- All updates are cumulative
- Infrequent, every 2-3 years



Options to control update behavior

- OEMs and Enterprises have several options to control update behavior

- Define update behavior through policy and maintenance windows
  - Control download, install and reboot

- Devices can connect directly to Windows Update (WU)

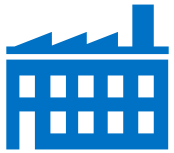
- Enterprises can further control update through Windows Server Update Services (WSUS)

Activation Options for Windows 10 IoT Enterprise

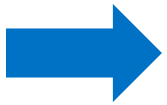
Direct OEMs	OA3.0 5x5 Multi Activation key (ePKEA) 5x5 Single Activation key (PKEA)
Channel OEMs	5x5 Multi Activation key (ePKEA) 5x5 Single Activation key (PKEA)

Flexibility creating devices with online and deferred activation options

Activation States for Windows 10 IoT Enterprise



Windows Product Key is injected or installed into each device during manufacturing



Device deployment

Has never connected to the Internet

Differed Activation

- *Image is fully functional*
- *No access to MSFT and/or 3rd party services*
- *No disruptive activation notifications or watermarks*

Internet connectivity

- *Device will reach AVS server for activation*
- *Upon successful activation access to online services*

Note: Activation failure UX will be appear if activation fails

Windows 10 IoT Enterprise – Activation UI

Device has never connected to the Internet

Deferred Activation

Windows activation

Connect to the Internet to activate Windows. Read the Microsoft Software License Terms

Product ID: 00360-20000-00002-AA921 Activate Windows

Device has Internet connectivity

Successful Activation

Windows activation

Windows is activated Read the Microsoft Software License Terms

Product ID: 00360-20000-00002-AA921 Change product key

Activation Failure

Windows activation

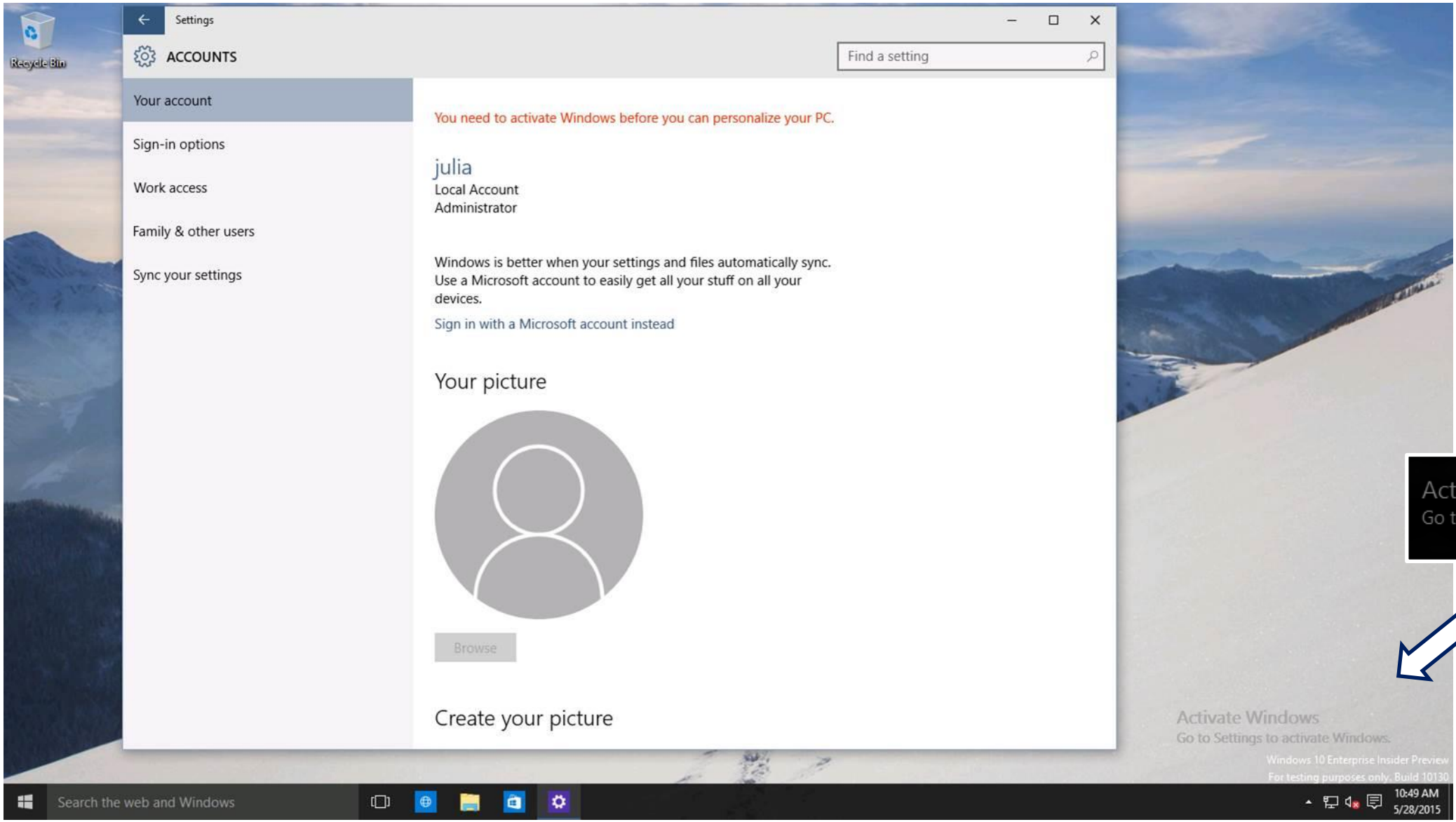
Windows is not activated. Read the Microsoft Software License Terms

Product ID: 00308-40000-00001-AAOEM Activate Windows

Activate Windows

Go to Settings to activate Windows.

Windows is not Activated - Personalization



Activate Windows
Go to Settings to activate Windows.

Windows 10 IOT Enterprise highlights

Windows 10 IoT Enterprise Entry	Windows 10 IoT Enterprise Value	Windows 10 IoT Enterprise High End

- One product key ePKEA for 50,000 installations
- Devices not connected to the Internet - remain in a deferred activation state

Microsoft Azure IoT Services

Devices	Device Connectivity	Storage	Analytics	Presentation & Action
	Event Hubs	SQL Database	Machine Learning	App Service
	Service Bus	Table/Blob Storage	Stream Analytics	Power BI
	External Data Sources	DocumentDB	HDInsight	Notification Hubs
		External Data Sources	Data Factory	Mobile Services
				BizTalk Services

Thank you for your attention ☺